






|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
|   | Página  | 1        | de      | 65  |      |

## CONTENIDO


### Tabla de contenido

|  |    |
|--|----|
| 1. INTRODUCCIÓN.....   | 4  |
| 2. JUSTIFICACIÓN.....  | 5  |
| 3. OBJETIVO .....  | 5  |
| 4. ALCANCE .....   | 5  |
| 4.1. Alcance/Aplicabilidad.....  | 5  |
| 4.2. Beneficios.....   | 5  |
| 4.3. Nivel de cumplimiento .....   | 5  |
| 5. TERMINOS Y DEFINICIONES.....  | 5  |
| 6. GENERALIDADES .....   | 12 |
| 6.1. Importancia de los Manuales de Normas y Políticas.....                                | 13 |
| 6.2. Comunicación y Socialización de las Políticas .....                                   | 13 |
| 6.3. Incumplimiento de las Políticas de Seguridad .....                                    | 13 |
| 6.4. Revisión de las Políticas.....  | 13 |
| 6.5. Responsables y Roles.....   | 13 |
| 6.6. Servicios Ofrecidos por los Sistemas de Información y la Plataforma Tecnológica ..... | 15 |
| 6.7. Almacenamiento en la Red.....   | 15 |
| 6.8. Consideraciones de Software .....   | 15 |
| 6.9. Correo Electrónico .....  | 15 |
| 6.10. Acceso a Internet.....   | 15 |
| 6.11. Consideraciones de una red .....   | 16 |
| 6.12. Impresión en red.....  | 16 |
| 7. MARCO LEGAL.....  | 16 |
| 8. IMPACTO.....  | 16 |
| 9. POLÍTICAS .....   | 17 |


| ELABORÓ  |     |      | REVISÓ Y SUBIO AL SIG:   |     |      | APROBÓ:   |     |     |      |
|--|-----|------|--|-----|------|---|-----|-----|------|
| DIEGO HERNANDO ZULUAGA SERNA   |     |      | JUAN DAVID MARULANDA ALVAREZ   |     |      | OSCAR JOSE FRANCO ECHAVARRIA  |     |     |      |
| <br>PERSONERÍA DE MEDELLÍN<br>DICCIONARIO DE VALORES S.G.C. |     |      | <br>PERSONERÍA DE MEDELLÍN<br>DICCIONARIO DE VALORES S.G.C. |     |      |  |     |     |      |
| FIRMA  |     |      | FIRMA  |     |      | FIRMA   |     |     |      |
| DIA  | MES | AÑO  | DIA  | MES | AÑO  | NRO. RESOLUCION   | DIA | MES | AÑO  |
| 8  | 9   | 2021 | 8  | 9   | 2021 | 320   | 8   | 9   | 2021 |

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 2   | de       | 65      |     |      |

|   |    |
|---|----|
| 9.1. Política General de Seguridad y Privacidad de la Información .....                                 | 17 |
| 9.2. Organización de la Seguridad de la Información .....   | 18 |
| 9.2.1. Organización interna .....   | 18 |
| 9.2.2. Política para dispositivos móviles .....   | 18 |
| 9.2.3. Política para el Teletrabajo .....   | 19 |
| 9.3. Seguridad de los Recursos Humanos .....  | 20 |
| 9.3.1. Antes de asumir el empleo .....  | 21 |
| 9.3.2. Durante la ejecución de la labor .....   | 21 |
| 9.3.3. Desvinculación de contratistas y licencias, vacaciones o cambio de labores de funcionarios ..... | 22 |
| 9.4. Gestión de Activos .....   | 22 |
| 9.4.1. Responsabilidad sobre los activos .....  | 23 |
| 9.4.2. Clasificación de la información .....  | 24 |
| 9.4.3. Manejo de los soportes de almacenamiento .....   | 25 |
| 9.5. Control de accesos .....   | 26 |
| 9.5.1. Política de control de accesos .....   | 26 |
| 9.5.2. Gestión de acceso de usuarios .....  | 27 |
| 9.5.3. Responsabilidades de los usuarios .....  | 28 |
| 9.5.4. Control de Acceso a Sistemas de Información y Aplicaciones .....                                 | 29 |
| 9.6. Cifrado .....  | 31 |
| 9.7. Seguridad Física y Ambiental .....   | 31 |
| 9.7.1. Áreas seguras .....  | 32 |
| 9.7.2. Seguridad de los equipos .....   | 33 |
| 9.7.3. Política de puesto de trabajo despejado y bloqueo de pantalla .....                              | 35 |
| 9.8. Seguridad de las Operaciones .....   | 36 |
| 9.8.1. Responsabilidades y procedimientos de operación .....  | 37 |
| 9.8.2. Protección contra Códigos Maliciosos .....   | 38 |
| 9.8.3. Copias de seguridad .....  | 39 |
| 9.8.4. Registro de actividad y supervisión .....  | 41 |

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 3   | de       | 65      |     |      |

|   |    |
|---|----|
| 9.8.5. Control del software en explotación.....   | 42 |
| 9.8.6. Gestión de Vulnerabilidad Técnica .....  | 43 |
| 9.9. Seguridad en las Telecomunicaciones.....   | 44 |
| 9.9.1. Gestión de la seguridad en las redes.....  | 44 |
| 9.9.2. Políticas y procedimientos de transferencia de información .....                       | 45 |
| 9.9.3. Políticas y procedimientos de uso del correo electrónico.....                          | 46 |
| 9.9.4. Política de uso adecuado de internet.....  | 50 |
| 9.10. Adquisición, Desarrollo y Mantenimiento de Sistemas.....                                | 53 |
| 9.10.1. Establecimiento de los requisitos de seguridad de los sistemas de información .....   | 53 |
| 9.10.2. Seguridad en los procesos de desarrollo y soporte.....                                | 54 |
| 9.10.3. Datos de prueba .....   | 56 |
| 9.11. Seguridad de la información en las relaciones con los proveedores o terceros .....      | 57 |
| 9.11.1. Política de seguridad de la información para las relaciones con los proveedores ..... | 57 |
| 9.11.2. Gestión de la prestación de servicios de proveedores.....                             | 58 |
| 9.12. Gestión de Incidentes de Seguridad de la Información.....                               | 59 |
| 9.12.1. Gestión de incidentes y mejoras en la seguridad de la información.....                | 59 |
| 9.13. Seguridad de la Información en la Gestión de la Continuidad del Negocio .....           | 60 |
| 9.13.1. Continuidad de seguridad de la información.....                                       | 60 |
| 9.14. Cumplimiento.....   | 62 |
| 9.14.1. Cumplimiento de requisitos legales y contractuales.....                               | 62 |
| 9.14.2. Revisiones de seguridad de la información.....  | 63 |
| 9.14.3. Privacidad y protección de información de datos personales .....                      | 63 |
| ACTUALIZACION DE LAS POLITICAS DE USO Y MANEJO DE INFORMACIÓN .....                           | 64 |

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 4   | de       | 65      |     |      |

## 1. INTRODUCCIÓN


Actualmente la seguridad de la información ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes para explorar más allá de las fronteras, situación que ha llevado a la aparición de nuevas amenazas en los sistemas de información. Como son los virus, el robo, los casos fortuitos o pérdida de información. Esto nos lleva a implementar procedimientos, políticas y normas que orienten en el uso adecuado de los Sistemas de Información y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la misma, lo cual puede ocasionar serios problemas en los bienes y servicios que posee la Personería de Medellín.

De acuerdo con la Resolución 054 del 13 de febrero de 2019 en donde se conforma el Comité de Seguridad de la Información (CSI) de la Personería de Medellín que formulará y recomendará a la Alta Dirección la adopción de Políticas de Seguridad de la Información y procedimientos para el adecuado uso de los sistemas de información, recursos informáticos y físicos, para asegurar que la información de la Personería de Medellín se encuentre protegida, impulsado la implementación del Sistema de Gestión de Seguridad de la Información. Es integrado por el Personero Auxiliar, el jefe de la oficina Asesora de Planeación, el líder de la oficina de Gestión Jurídica, el jefe de la oficina de Control Interno, el Personero Delegado para la Atención al Público y un profesional Personería Auxiliar (Gestión de Informática).

En este sentido, las políticas de seguridad de la información deben surgir como una herramienta para concientizar a cada uno de los miembros de la Personería de Medellín sobre la importancia y sensibilidad de la información y servicios críticos que permiten desarrollarse y mantenerse en su sector.

Las políticas de seguridad de la información constituyen las alarmas y compromisos compartidos de la Personería de Medellín, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí solas no constituyen una garantía para la seguridad de la Personería de Medellín, ellas deben responder a intereses y necesidades que se poseen basadas en la visión, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad de la información factores que facilitan la formalización y materialización de los compromisos adquiridos con la Personería de Medellín.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 5   | de       | 65      |     |      |

## 2. JUSTIFICACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Personería de Medellín con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

## 3. OBJETIVO

Establecer las políticas de seguridad de la información para la Personería de Medellín, de acuerdo con los lineamientos de buenas prácticas en seguridad para las Entidades del estado con el fin de preservar la confidencialidad, integridad y disponibilidad de la información en la Entidad.

## 4. ALCANCE

### 4.1. Alcance/Aplicabilidad

Con el manual, se describen las políticas y estándares informáticos para todos los usuarios de la Personería de Medellín que tienen a su cargo recursos informáticos, orientarlos a alcanzar los logros institucionales e informarles de las políticas que deben aplicar para el buen uso de los equipos de cómputo, aplicaciones y demás servicios informáticos.

### 4.2. Beneficios


El manual beneficiará a todos los usuarios que utilizan los servicios informáticos de la Entidad, ya que las políticas y estándares en materia Informática son la base del buen funcionamiento, desempeño, seguridad y protección de los activos tecnológicos del Instituto.

### 4.3. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

## 5. TERMINOS Y DEFINICIONES

**Acuerdos de Niveles de Servicio:** Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. Es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 6   | de       | 65      |     |      |

como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, entre otros.<sup>1</sup>

**Activo de información:** Cualquier componente (tecnológico, software, documento o de infraestructura) que soporta uno o más procesos de negocios y en consecuencia debe ser protegido. Además los activos de información son el resultado de la construcción de un inventario y clasificación que posee la Entidad de acuerdo con la Política General de Seguridad y Privacidad de la Información, la cual determina que activos posee la Entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos.<sup>2</sup>

**Amenazas:** Las amenazas pueden desencadenar o explotar una vulnerabilidad para comprometer algún aspecto del activo. Son externas a los activos de información. La identificación de amenazas y vulnerabilidades en #ISO27001 es esencial para una gestión de riesgos adecuada.<sup>3</sup>

**Análisis de riesgos de seguridad de la información:** Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.<sup>4</sup>

**Aplicaciones o aplicativos:** Las aplicaciones son herramientas Informática s que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

**Autenticación:** Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales.<sup>5</sup>

**Autorización:** Consentimiento expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

**Backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

**Base de datos:** Todo conjunto organizado de datos personales que sea objeto de tratamiento


<sup>1</sup> <https://www.ticportal.es/glosario-tic/acuerdo-nivel-servicio-ans>

<sup>2</sup> <https://mintic.gov.co/portal/inicio/Transparencia-y-acceso-a-informacion-publica/Instrumentos-de-Gestion-de-Informacion-Publica/80628:10-2-Registro-de-Activos-de-Informacion>

<sup>3</sup> <https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/>

<sup>4</sup> [https://www.mintic.gov.co/gestionti/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf)

<sup>5</sup> Norma Técnica Colombiana, NTC-ISO 3270

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 7   | de       | 65      |     |      |

**Centro de Datos:** Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

**Cifrado:** Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.<sup>6</sup>

**Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.<sup>7</sup>

**Cookies:** es un término que hace referencia a una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador. Las cookies son utilizadas habitualmente por los servidores de aplicaciones para diferenciar usuarios y para actuar de diferente forma dependiendo de estos.<sup>8</sup>

**Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, Entidades o procesos no autorizados.<sup>9</sup> Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, Entidades o procesos autorizados.

**Contenido:** Todo tipo de información o dato que se divulga en la intranet y/o página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños y animaciones.<sup>10</sup>

**Contraseña o clave de autenticación:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

**Copyright:** Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.<sup>11</sup>

<sup>6</sup> <https://latam.kaspersky.com/resource-center/definitions/encryption>


<sup>7</sup> <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/5482:Sistemas-de-Gestion-de-la-Seguridad-de-la-Informacion-SGSI>

<sup>8</sup> [https://es.wikipedia.org/wiki/Cookie\\_\(inform%C3%A1tica\)#Prop%C3%B3sito](https://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)#Prop%C3%B3sito)

<sup>9</sup> [NTC 5411-1:2006]

<sup>10</sup> <https://www.inbuze.com/contenidos-digitales>

<sup>11</sup> <https://dudas.derechosdigitales.org/caso/que-significa-el-simbolo-copyright-es-obligatorio-su-uso/>

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 8   | de       | 65      |     |      |

**Custodio:** Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.<sup>12</sup>

**Dato personal:** toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional.<sup>13</sup>

**Datos o información sensibles:** Se entiende como datos sensibles aquellos que afecten la intimidad del titular o cuyo uso indebido pueda afectar la intimidad del titular o la potencialidad de generar su discriminación.<sup>14</sup>

**Datos públicos:** Es el dato que la ley o la Constitución Política determina como tal, o aquellos datos que no sean semiprivados, privados o sensibles. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o servidor público.<sup>15</sup>

**Dato Semiprivado:** Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.<sup>16</sup>

**Dato Privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.<sup>17</sup>

**Dirección IP:** La dirección IP o Internet Protocol es un número único e irreplicable con el que se identifica un computador conectado a una red que corre el protocolo IP.<sup>18</sup>

**Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.<sup>19</sup>

<sup>12</sup> <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/5482:Sistemas-de-Gestion-de-la-Seguridad-de-la-Informacion-SGSI>

<sup>13</sup> <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

<sup>14</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data\\_es](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data_es)


<sup>15</sup> <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

<sup>16</sup> <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

<sup>17</sup> <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

<sup>18</sup> <http://blog.orange.es/innovacion/que-es-direccion-ip-y-que-tenes-que-saber-sobre-la-tuya/>

<sup>19</sup> [NTC 5411-1:2006]

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 9   | de       | 65      |     |      |

**Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de la red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red. Es la parte principal de una dirección en la web, que usualmente indica la organización o compañía que administra dicha web.<sup>20</sup>

**Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.<sup>21</sup>

**Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.<sup>22</sup>

**Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.<sup>23</sup>

**Internet:** Herramienta de comunicación con decenas de miles de redes de computadoras unidas Internet global consiste en decenas de miles de redes interconectadas operadas por proveedores de servicios, compañías individuales, universidades, gobiernos y otros.<sup>24</sup>

**Intranet:** Es una red de computadores o terminales privados similar a internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.<sup>25</sup>

**Incidente de seguridad:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).<sup>26</sup>

<sup>20</sup> [https://es.wikipedia.org/wiki/Dominio\\_de\\_Internet](https://es.wikipedia.org/wiki/Dominio_de_Internet)

<sup>21</sup> <https://www.sic.gov.co/preguntas-frecuentes->

[pdp#:~:text=El%20Responsable%20del%20Tratamiento%20de,personales%20por%20cuenta%20del%20Responsable.](#)


<sup>22</sup> [Guía ISO/IEC 73:2002]

<sup>23</sup> [NTC 5411-1:2006]

<sup>24</sup> <https://www.internetsociety.org/es/internet/>

<sup>25</sup> <https://www.tecnologia-informatica.com/que-es-una-intranet/>

<sup>26</sup> [ISO/IEC TR 18044:2004]

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 10  | de       | 65      |     |      |

**Integridad:** Es la protección de la exactitud y estado completo de los activos.<sup>27</sup>

**Inventario de activos de información:** es una lista ordenada y documentada de los activos de información perteneciente a la Entidad.

**Licencia de software:** Es un contrato entre el autor del programa y el usuario, en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.<sup>28</sup>

**Log de auditoría:** Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

**Medio de almacenamiento físico:** Son dispositivos capaces de grabar datos en su memoria, facilitando así, el transporte de información y la distribución de esta en distintos equipos. como las cintas, los discos extraíbles, los DCs y los DVDs entre otros.<sup>29</sup>

**Parche o Actualización:** los parches generalmente corrigen pequeños errores al tiempo que mantienen la compatibilidad del software. El aumento en el número de parches ocurre cuando realiza correcciones de errores compatibles con versiones anteriores. Es una actualización para una pieza de software o programa para corregir un bug o una vulnerabilidad, y para mejorarlo.<sup>30</sup>

**Portal web:** Es un sitio compuesto por varias páginas web, el cual, permite a las personas el fácil acceso a diferentes recursos y servicios en línea que se ofrece.<sup>31</sup>

**Perfiles de usuario:** Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información, a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

**Propietario del activo de información:** es la dependencia, cargo, grupo de trabajo o proceso donde se crean los activos de información y tiene la responsabilidad de garantizar que la información y los activos asociados de procesamiento de información se clasifican adecuadamente, y de definir y


<sup>27</sup> [NTC 5411-1:2006]

<sup>28</sup> <https://www.tecnologia-informatica.com/tipos-licencias-software-libre-comercial/>

<sup>29</sup> <https://www.tecnologia-informatica.com/dispositivos-de-almacenamiento-informacion/>

<sup>30</sup> <https://www.welivesecurity.com/la-es/2017/07/14/parches-y-actualizaciones-microsoft-wannacryptor/>

<sup>31</sup> <https://www.liferay.com/es/resources/l/web-portal>

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 11  | de       | 65      |     |      |

revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.<sup>32</sup>

**Red de datos:** Una red de datos es un conjunto de computadores que están conectados entre sí compartiendo recursos, información, y servicios.<sup>33</sup>

**Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.<sup>34</sup>

**Servicio de TI:** Un servicio de tecnologías de la información es un conjunto de productos que buscan solucionar las necesidades de los clientes de una organización a través del uso de elementos tecnológicos o informáticos.

**Servidor:** Computador central en un sistema de red que provee servicios a otras computadoras.<sup>9</sup>  
**Sistema Informático o de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos.<sup>35</sup>

**Sistema de información:** Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Personería de Medellín o de origen externo, ya sea adquirido por el Instituto como un producto estándar de mercado o desarrollado para las necesidades de éste.

**Sistema de Gestión de Seguridad de la Información (SGSI):** Sistema de Gestión de la Seguridad de la Información parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.<sup>36</sup>

**Software malicioso:** Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o


<sup>32</sup> <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/5482:Sistemas-de-Gestion-de-la-Seguridad-de-la-Informacion-SGSI>

<sup>33</sup> <https://searchdatacenter.techtarget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias>

<sup>34</sup> [NTC-ISO/IEC 17799:2006]

<sup>35</sup> <https://desafiohosting.com/que-es-un-servidor/>

<sup>36</sup> NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 12  | de       | 65      |     |      |

sistemas de información.

**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales como la recolección, almacenamiento, uso, circulación o supresión.<sup>37</sup>

**Tratamiento del Riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.<sup>38</sup>

**Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.

**Usuario:** Cualquier persona, Entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.<sup>39</sup>

**Vulnerabilidades:** una vulnerabilidad de seguridad es una debilidad en el hardware o el software (un bug o error de programación) que puede explotarse para poner en peligro los sistemas y dar a los atacantes acceso a sus datos e información.<sup>40</sup>

## 6. GENERALIDADES

La información presentada en el siguiente manual ha sido elaborada de maneja sencilla de tal manera que pueda ser interpretada por cualquier persona que labore para la Personería de Medellín, con o sin conocimientos informáticos.

Las políticas fueron creadas obedeciendo a las necesidades y en el entorno operacional en donde se identificaron problemáticas y previniendo futuras rupturas en la seguridad, aplicados a los diferentes activos y recursos de la Personería de Medellín.


Los diferentes niveles de seguridad fueron desarrollados con base a la situación real de la Personería de Medellín, elaborando cada política con sumo cuidado sobre qué activo proteger, de qué protegerlo como protegerlo y por qué protegerlo; los mismos se organizan siguiendo el esquema, normativo de seguridad, ISO/IEC 27001 (mejores prácticas de seguridad).

<sup>37</sup> NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

<sup>38</sup> NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

<sup>39</sup> <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/5482:Sistemas-de-Gestion-de-la-Seguridad-de-la-Informacion-SGSI>

<sup>40</sup> <https://es-la.tenable.com/vulnerability-management>

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 13  | de       | 65      |     |      |

### 6.1. Importancia de los Manuales de Normas y Políticas

Como parte integral de un Sistema de Gestión de Seguridad de la Información (SGSI), un manual de normas y políticas de seguridad trata de definir; qué, por qué, de qué y cómo se debe proteger la información. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la Personería de Medellín. Estos documentos tratan a su vez de ser el medio de interpretación de la seguridad para toda la organización.

### 6.2. Comunicación y Socialización de las Políticas

Todo funcionario o contratista que ingrese a la Personería de Medellín deberá recibir capacitación sobre las políticas establecidas en el presente manual en el momento de su inducción. La Personería Auxiliar (Gestión del Talento Humano) remitirá con la debida anticipación al Personería Auxiliar (Gestión de Informática), la información de fecha, hora y lugar de las jornadas de inducción sobre las políticas de seguridad en la información.

### 6.3. Incumplimiento de las Políticas de Seguridad

El incumplimiento de las políticas establecidas en el presente manual podrá acarrear sanciones disciplinarias, civiles o penales según sea el caso.

### 6.4. Revisión de las Políticas


El Manual del Sistema de Gestión de Seguridad de la Información es revisado anualmente o antes de ser necesario, con el fin de mantenerlo actualizado y acorde a los cambios en la infraestructura tecnológica, los procedimientos y servicios que involucran el manejo de la información institucional.

### 6.5. Responsables y Roles

Además del Comité de Seguridad de la Información (CGI), existen varios grupos de personas que interactuarán con los sistemas de información y la plataforma tecnológica, los cuales por sus funciones en la Personería de Medellín tienen diferentes responsabilidades y permisos frente al sistema.

- **Comité de Seguridad de la Información - CGI**

De acuerdo con la Resolución 054 del 13 de febrero de 2019 en donde se conforma el Comité de Seguridad de la Información (CSI) de la Personería de Medellín que formulará y recomendará a la Alta Dirección la adopción de Políticas de Seguridad de la Información y procedimientos para el adecuado uso de los sistemas de información, recursos informáticos y físicos, para asegurar que la información de la Personería de Medellín se encuentre protegida, impulsado la implementación del Sistema de Gestión de Seguridad de la Información. Es integrado por el Personero Auxiliar, el jefe de la oficina Asesora de Planeación, el líder de la oficina de Gestión Jurídica, el jefe de la oficina de Control Interno, el Personero Delegado para la Atención al Público y un profesional del

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 14  | de       | 65      |     |      |

Personería Auxiliar (Gestión de Informática) . Entre las funciones que tiene el CGI se encuentran las siguientes:

- Coordinar la implementación del Manual del Sistema de Gestión de Seguridad de la Información al interior de la Entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en la Personería de Medellín.
- Acompañar e impulsar el desarrollo de proyectos de seguridad de la información.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Personería de Medellín

- **Líderes de Aplicaciones y/o Responsables de los Procesos y/o Directores o Jefes de dependencias u oficinas**

Es el responsable de las aplicaciones y de velar por la calidad de los datos que hacen parte del sistema de información. Esta responsabilidad está asignada por aplicaciones, y generalmente el responsable corresponde con el jefe de la dependencia o líder del proceso a quien pertenece la información (Penal, Vigilancia, Personería Auxiliar, Disciplinarios, Protección del Interés Público, Atención al Público, oficina Asesora de Planeación, Control Interno, oficina Asesora de Comunicaciones, oficina de Gestión del Talento Humano, Gestión Financiera, Gestión Contractual, Gestión de Archivo entre otros)


Informar al Personería Auxiliar (Gestión de Informática) las novedades de los funcionarios y contratistas, así como los permisos de las carpetas o recursos compartidos para los cuales están autorizados. Conocer, promover y asegurar la ejecución y cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo dentro de sus dependencias.

- **Personería Auxiliar - Personería Auxiliar (Gestión de Informática)**

Es responsable de velar por el correcto funcionamiento de los sistemas de información. Liderar las actividades relacionadas con la implementación, mantenimiento y mejora continua de las Políticas de Seguridad de la Información en la Personería de Medellín, garantizando la divulgación y el seguimiento de las políticas de seguridad de la información al interior de la Entidad, estableciendo los procedimientos, lineamientos y controles que permitan su operatividad y cumplimiento.

- **Funcionarios, Contratistas y Terceros**

Tienen acceso a los sistemas de información. Cada funcionario tiene un nombre de usuario, que corresponde a las iniciales de los nombres con el primer apellido; también tiene una contraseña, además posee unos permisos o autorizaciones dentro del sistema para realizar las funciones asignadas por la institución.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 15  | de       | 65      |     |      |

Conocer y aplicar los procedimientos de seguridad de la información y proteger el buen manejo de la información física y digital, a riesgo de incidir en faltas contractuales y/o disciplinarias. Reportar oportunamente las falencias e incidentes de seguridad que descubra y proteger el acceso a los recursos informáticos asignados, a través de contraseñas seguras. Debe concluir las sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados al retirarse del puesto de trabajo. Aceptar la responsabilidad por el manejo del espacio en disco de su computador de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

#### **6.6. Servicios Ofrecidos por los Sistemas de Información y la Plataforma Tecnológica**

La razón de ser de los sistemas de información es ofrecer servicios a los usuarios. Cada uno de los servicios que presta el sistema incurre en unos riesgos propios, que deben ser valorados y analizados profundamente, como parte de una definición amplia de políticas de seguridad, y posterior generación de un plan de contingencias que nos permita regenerar el sistema completo, o parte de él, en caso de un evento catastrófico, bien sea natural, vandálico o fortuito, y el cual puede afectar el hardware, el software o el entorno físico del sistema de información. Estos servicios generan cada uno diferentes requisitos para acceder a ellos, por lo que cada uno se describirá brevemente y de manera independiente.

#### **6.7. Almacenamiento en la Red**

Los usuarios de la Personería de Medellín están autorizados para guardar información en la red, de acuerdo con una distribución por grupos de usuarios, normalmente por procesos. Existen espacios en la red completamente privados o restringidos para cierto grupo de usuarios, y otros públicos que pueden ser accedidos por muchas personas e incluso por todas las que tienen acceso a la red.

#### **6.8. Consideraciones de Software**


Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia de este (el software pirata o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

#### **6.9. Correo Electrónico**

Esta herramienta está habilitada en la actualidad para los usuarios de la red y permite comunicarse interna y externamente, de igual manera el correo puede ser accedido internamente, o desde fuera de la Personería de Medellín vía internet.

#### **6.10. Acceso a Internet**

El acceso a internet permite que usuarios internos de la red puedan acceder a todos los servicios que Internet provee y solo se podrá consultar información de carácter institucional.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 16  | de       | 65      |     |      |

### 6.11. Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de computadores ajenos, como portátiles. Mantener al máximo el número de recursos de red en sólo en modo lectura impide que computadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo. Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas. Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

### 6.12. Impresión en red

Algunos usuarios tienen impresoras locales en sus computadores, pero otros imprimen archivos en impresoras de red; siendo este servicio de uso restringido

## 7. MARCO LEGAL


- La elaboración del manual de normas y políticas de seguridad Informática está fundamentada bajo la norma ISO/IEC 27001.
- Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.
- Ley 1273 de 2009 “Protección de la Información y de los Datos”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.

## 8. IMPACTO

Generalmente la puesta en marcha de una política de seguridad se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los funcionarios de la Personería de Medellín tienen sólo los permisos que se les dio.

La seguridad de la información debe ser estudiada para que no impida el trabajo de los funcionarios en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, requiere:

- Elaborar reglas y procedimientos para cada servicio de la organización sin que el trabajo de los funcionarios y contratistas corra riesgos o se vea afectado.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 17  | de       | 65      |     |      |

- Sensibilizar a los funcionarios y contratistas con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los funcionarios deben ser definidos por los responsables jerárquicos (jefes) y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida por la Personería de Medellín. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los funcionarios sobre problemas y recomendaciones en término de seguridad.


## 9. POLÍTICAS

### 9.1. Política General de Seguridad y Privacidad de la Información

La Personería de Medellín entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la Personería de Medellín la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros, aprendices, practicantes y usuarios de Personería de Medellín
- Garantizar la continuidad del negocio frente a incidentes.
- Personería de Medellín ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 18  | de       | 65      |     |      |

las necesidades del negocio, y a los requerimientos regulatorios.

Basados en las responsabilidades de los diferentes actores del sistema (usuarios, líderes de aplicaciones y administradores del sistema de información) y en la plataforma tecnológica existente se definen unas políticas para el uso racional de los recursos informáticos, las cuales han sido aprobadas por la alta dirección de la Personería de Medellín y son de obligatorio cumplimiento para todas las personas que tienen acceso al sistema de información.


## 9.2. Organización de la Seguridad de la Información

### 9.2.1. Organización interna

- La Personería Auxiliar (Gestión de Informática) deberá identificar las autoridades pertinentes hacia quienes pueda acudir en el caso de que un incidente de seguridad lo amerite; y debe mantener contacto con grupos de interés especial del ámbito de la seguridad de la información que aporten a la gestión de los riesgos de seguridad identificados en la Personería de Medellín.
- Los responsables de los procesos y/o supervisores del contrato definirán los roles de usuario que estimen pertinentes en cada uno de sus equipos de trabajo y los niveles de operación en los sistemas de información y la plataforma tecnológica.
- Los proyectos que desarrolle la Personería de Medellín deberán estar alineados a las políticas de seguridad contenidas en el presente manual, deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- Las actividades y proyectos encaminados a la gestión de la seguridad de la información deberán estar enmarcados en la estrategia de la Personería de Medellín y alineados al cumplimiento de las funciones misionales de la institución.

### 9.2.2. Política para dispositivos móviles


Personería Auxiliar (Gestión de Informática) será la responsable de establecer las condiciones necesarias para el acceso a los recursos y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, smartphones, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes). La autorización de conexión de dispositivos móviles a las redes de datos de la Personería de Medellín se realiza una vez se identifican, gestionan y mitigan los riesgos de seguridad de la información asociados al uso de los dispositivos.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 19  | de       | 65      |     |      |

- La presente política y controles aplicarán a todos los dispositivos y equipos móviles de los funcionarios, contratistas y terceros, que estén autorizados para conectarse a las redes de datos y comunicaciones de la Personería de Medellín, a la información institucional o a cualquier servicio de tecnologías de la información y comunicación de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) deberá disponer de un mecanismo de conexión seguro que garantice que las conexiones de teletrabajo autorizadas por la Personería de Medellín se realizan de forma segura y se protegen los activos de información en uso.
- Personería Auxiliar (Gestión de Informática) implementará y adoptará los mecanismos de seguridad necesarios para proteger la información contenida y transmitida por medio del uso de dispositivos móviles de los funcionarios, contratistas y terceros de la Personería de Medellín.
- Los dispositivos móviles que hagan uso de información de la Personería de Medellín o que se conecten a su red se deberán acoger a las políticas de seguridad de la información definidas en el presente manual.
- Al conectar un dispositivo a la red de la Personería de Medellín, el propietario del dispositivo aceptará las políticas definidas en el presente manual y así mismo, las disposiciones que estas determinen.
- Los dispositivos móviles solo tienen acceso a la información autorizada por parte de los responsables de los diferentes procesos de la Personería de Medellín.
- Los usuarios se comprometen a proteger física y lógicamente los dispositivos móviles asignados e inventariados por la oficina del Personería Auxiliar (Gestión de Bienes Logísticos) que son propiedad de la Personería de Medellín, para prevenir el hurto, acceso o divulgación no autorizada de la información institucional.
- Personería Auxiliar (Gestión de Informática) estará autorizada para realizar la desactivación, borrado y retiro de los accesos de los dispositivos móviles a los sistemas de información de la Personería de Medellín y demás servicios de tecnología, cuando el dispositivo móvil haya sido extraviado, hurtado o haya sido comprometida su seguridad.

### 9.2.3. Política para el Teletrabajo

La Personería de Medellín deberá velar por garantizar la seguridad de la información, así como de los equipos y los teletrabajadores, dado que se trasladan numerosos datos y contenidos a dispositivos electrónicos con nuevas y diferentes ubicaciones físicas generando nuevos riesgos que se deben mitigar estableciendo protocolos adecuados. Estas políticas de seguridad se instauran como planes

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 20  | de       | 65      |     |      |


de acción encargados de afrontar, aminorar y prevenir los riesgos originados con la implementación del teletrabajo.

- Personería Auxiliar (Gestión de Informática) deberá disponer de un mecanismo de conexión seguro que garantice que las comunicaciones digitales de teletrabajo autorizadas por la Personería de Medellín se realizan de forma segura y se protegen los activos de información usados.
- Como la información se considera como el recurso intangible de mayor importancia Personería Auxiliar (Gestión de Informática) deberá prevenir cualquier anomalía estableciendo servicios de antivirus, respaldo o backup, acceso seguro a través de VPN (Virtual Private Network - Red Privada Virtual) y acceso restringido a aplicaciones. La definición de las políticas de seguridad debe garantizar:
  - Confidencialidad: asegurar el acceso a la información por las personas únicamente autorizadas, es decir, los teletrabajadores.
  - Integridad: garantizar los datos libres de modificaciones no autorizadas.
  - Disponibilidad: certificar que la información esté a la disposición de los teletrabajadores en cualquier momento, para que puedan desarrollar sus actividades.
  - Autenticación: identificar al usuario generador de la información.
- Personería Auxiliar (Gestión de Informática) deberá orientar por reducir las amenazas de los recursos intangibles, también se deben establecer los procedimientos de la protección de los recursos tangibles a través de un análisis de riesgos ocasionados por la implementación de teletrabajo, por ejemplo, establecer procesos de manejo de equipos, pólizas de seguros, mantenimiento de equipos, entre otros.

### 9.3. Seguridad de los Recursos Humanos

La Personería de Medellín reconoce la importancia del factor humano para el cumplimiento de los objetivos misionales y con el interés de tener el mejor personal calificado, garantizará que la vinculación de nuevos funcionarios y contratistas se realizará siguiendo un proceso formal de selección de acuerdo con la legislación actual, el cual estará orientado a las funciones y roles que deben desempeñar en el ejercicio de sus funciones. Las siguientes son las Políticas de Seguridad de la Información en la gestión de los Recursos Humanos que los funcionarios y contratistas deben conocer y aplicar. Para tener en cuenta la selección y contratación, la formación de funcionarios y contratistas, y la salida de la Entidad, de acuerdo con los procedimientos ya estipulados para tales fines.

El Personero, el Personero Auxiliar, los Personeros Delegados, así como los Jefes de oficina, son

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 21  | de       | 65      |     |      |


responsables de conocer y asegurar la implementación de las políticas de seguridad de la Información, dentro de sus dependencias, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

### 9.3.1. Antes de asumir el empleo

- Personería Auxiliar (Gestión del Talento Humano y Gestión Contractual) deberá realizar las actividades necesarias para la selección de personal, verificando los requisitos para proporcionar los cargos y el cumplimiento de la normas vigentes.
- Personería Auxiliar (Gestión del Talento Humano y Gestión Contractual) deberá contrastar los antecedentes para confirmar la veracidad de la información suministrada por el personal que va a ocupar un cargo, antes de su vinculación, de acuerdo con las leyes, reglamentos y ética vigentes en la Personería de Medellín y el país, como la Política de Tratamiento y Protección de Datos Personales.
- Para el ingreso de funcionarios y la suscripción de contratos o convenios relacionados con acceso a información institucional y/o servicios de tecnología, se deberá garantizar que la persona acepte y firme el Acuerdo de Confidencialidad y la aceptación de las Políticas de Seguridad de la Información de la Personería de Medellín, y se comprometa a mantener la confidencialidad de la información; este acuerdo se hará extensivo a todos los contratistas o terceros.

### 9.3.2. Durante la ejecución de la labor

- Personería Auxiliar (Gestión del Talento Humano y Gestión Contractual) y supervisores de contratistas serán los responsables de comunicar al Personería Auxiliar (Gestión de Informática) , las novedades de personal mediante el formato establecido.
- Los funcionarios y contratistas de la Personería de Medellín deberán reportar oportunamente las debilidades e incidentes de seguridad que detecten o que conozcan y proteger el acceso a los recursos informáticos asignados.
- Los responsables de los procesos, supervisores y jefes de oficinas deberán informar al Personería Auxiliar (Gestión de Informática) de los permisos a las carpetas o recursos compartidos de los funcionarios y contratistas para los cuales están autorizados.
- Todos los funcionarios y contratistas de la Personería de Medellín, deberán recibir inducción para formar, sensibilizar y se dar a conocer las políticas del presente manual, procedimientos y las obligaciones.
- La Personería de Medellín deberá mantener informado a todo el personal sobre los

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 22  | de       | 65      |     |      |

actualizaciones y cambios realizados a las políticas, procedimientos y al SGSI en general.

- Personería Auxiliar (Gestión de Informática) será el encargado de convocar a funcionarios y contratistas, a las charlas y eventos programados como parte del programa de sensibilización en Seguridad de la Información que será anual y así mismo deben proveer los recursos para su ejecución y controlar la asistencia.


### 9.3.3. Desvinculación de contratistas y licencias, vacaciones o cambio de labores de funcionarios

La Personería de Medellín asegurará que sus funcionarios y contratistas sean desvinculados o reasignados para la ejecución de nuevas labores de una forma controlada y segura.

- Los jefes de oficinas y supervisores serán responsables de custodiar la información institucional a cargo de funcionarios o contratistas cuando se produzca el retiro o suspensión de personal, o terminación o cesión de los contratos, llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
- Personería Auxiliar (Gestión del Talento Humano) será la responsable de informar al Personería Auxiliar (Gestión de Informática) , toda novedad de retiro, vacaciones, licencias o cambio de labores del personal.
- Personería Auxiliar (Gestión del Talento Humano) deberá asegurar que el abandono de la Entidad por parte de los funcionarios, contratistas o terceras personas es controlado, que se devuelven los equipos asignados y se eliminan completamente todos los derechos de acceso. Además deben informar al Personería Auxiliar (Gestión de Informática) para eliminar los accesos a todos los sistemas de información.
- Personería Auxiliar (Gestión del Talento Humano y Gestión de Bienes Logísticas) deberán tener actualizado y verificado regularmente el inventario de los activos cargados a cada funcionario con el fin de que al momento de la desvinculación la devolución de los activos de información o equipos sea más sencilla.


### 9.4. Gestión de Activos

La Personería de Medellín es propietaria tanto de los activos de información físicos y los generados, procesados, almacenados y transmitidos a través de los sistemas de información, y deberá otorgar responsabilidad a las dependencias sobre sus activos de información asegurando el cumplimiento de las directrices que regulen el uso adecuado de los mismos.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 23  | de       | 65      |     |      |

#### 9.4.1. Responsabilidad sobre los activos

- Todos los activos de información de la Entidad tendrán un responsable de acuerdo con la normatividad aplicable, con las directrices de Personería Auxiliar (Gestión de Bienes Logísticas).
- Toda la información contenida en los recursos informáticos de la Entidad es propiedad de la institución y ésta se reserva el derecho sobre sus diferentes usos. Es confidencial y de uso restringido dentro y fuera de la Entidad.
- Todo funcionario, contratista o tercero que haga uso de los recursos y sistemas de información de la Personería de Medellín, deberá tener acceso únicamente a la información estrictamente necesaria para el desempeño de las actividades que le han sido autorizadas.
- La información resultante de las actividades normales de la Entidad debe considerarse como un activo de información.
- Todos los funcionarios y contratistas de la Entidad deberán reportar a los responsables de sus dependencias o procesos o al Personería Auxiliar (Gestión de Informática) , cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de los activos de información de la Entidad.
- Personería Auxiliar (Gestión de Informática) es el propietario de los sistemas de información de la Entidad y por tanto deberá asegurar su operación y administración.
- Personería Auxiliar (Gestión de Informática y Gestión de Bienes Logísticos) deberán garantizar el levantamiento y actualización, activos de información tecnológicos.
- El designado por la Personería Auxiliar es quien deberá autorizar la instalación, cambios o eliminación de componentes de los sistemas de información y la plataforma tecnológica.
- Personería Auxiliar (Gestión de Informática) deberá establecer una configuración adecuada para los activos de información, con el fin de preservar la seguridad de la información y estandarizar las condiciones de uso.
- Todos los funcionarios, contratistas y terceros deberán usar los activos de información de forma ética y en cumplimiento de las leyes y reglamentos con el fin de evitar daños y pérdidas sobre la operación o la imagen de la Entidad.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 24  | de       | 65      |     |      |

- Si funcionarios, contratistas y terceros, necesitan instalar, hacer uso o compartir software (libre o propio) en los recursos proporcionados por la Entidad, deberán solicitar la autorización, verificación y registro del Personería Auxiliar (Gestión de Informática) .
- Todos funcionarios, contratistas y terceros deberán cumplir con los controles mínimos de seguridad establecidos (antivirus, sistema operativo con seguridad) por el Personería Auxiliar (Gestión de Informática) , para conectarse a las red de la Entidad.
- Si los funcionarios, contratistas y terceros necesitan utilizar equipos propios diferentes a los proporcionados por la institución, deberán solicitar la autorización, verificación y registro del Personería Auxiliar (Gestión de Informática) .
- Los funcionarios y contratistas deberán utilizar los recursos tecnológicos de la Entidad, con el único objetivo de llevar a cabo las labores asignadas al cargo; por consiguiente, no deben ser utilizados para fines ajenos a este.
- Todo funcionario o contratista deberá devolver los activos informáticos a su cargo, por retiro definitivo, cambio de puesto de trabajo, suspensión y/o finalización del contrato, haciendo entrega formal de los equipos a su cargo y las claves de acceso. Con las directrices del área de Personería Auxiliar (Gestión del Talento Humano y Gestión de Bienes Logísticos).

#### 9.4.2. Clasificación de la información

La Personería de Medellín definirá los niveles más adecuados para clasificar su información de acuerdo con su importancia y sensibilidad, y generará guías de clasificación de la información para que los propietarios puedan catalogarla y sea posible determinar controles específicos para su protección. El objetivo de la clasificación de la información es asegurar que se aplique un nivel de protección adecuado a cada activo de información

- Todos los activos inscritos a la información institucional serán identificados, clasificados y valorados, de acuerdo con lo establecido en las tablas de retención documental vigentes y a una metodología de gestión de activos formalmente adoptada.
- Toda información institucional deberá ser identificada, clasificada y documentada de acuerdo con la Guía de Clasificación de la Información o procedimiento formalmente establecido por la Entidad y las normas vigentes en un inventario de activos de información.
- Personería Auxiliar (Gestión Jurídica) deberá definir los niveles de clasificación de la información de la Entidad, orientar sobre los datos que son susceptibles de poner a disposición, sin que esto

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 25  | de       | 65      |     |      |


implique la vulneración de los derechos fundamentales de los individuos.

- Personería Auxiliar (Gestión de Informática) deberá implementar los mecanismos de control necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información que se encuentra en los recursos tecnológicos bajo su custodia.
- La información física y digital de la Entidad deberá tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o misionales. Este período debe ser indicado en las Tablas de Retención Documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada adecuadamente.
- Personería Auxiliar (Gestión de Informática) deberá establecer un inventario con el software y sistemas de información que se encuentran permitidos en las equipos de trabajo de la Entidad para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

#### 9.4.3. Manejo de los soportes de almacenamiento

La Personería de Medellín evitará la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento dispuestos para tal fin.

- Personería Auxiliar (Gestión de Informática) como responsable de proporcionar los medios, mecanismos o herramientas tecnológicas realizará la gestión de medios extraíbles de acuerdo con las necesidades de cada usuario respecto a las labores desempeñadas.
- Personería Auxiliar (Gestión de Informática) deberá implementar acciones, protocolos o procedimientos para el uso y administración de medios informáticos removibles.
- Los equipos de cómputo tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, deberán tener habilitado el escaneo automático de virus y tener configurado en el software de antivirus el bloqueo de la reproducción automáticas de archivos ejecutables.
- Personería Auxiliar (Gestión de Informática) deberá velar porque la información será eliminada de los medios de almacenamiento de forma segura cuando ya no sea necesaria, utilizando procedimientos y herramientas de borrado seguro, garantizando que no queden rastros de ésta.
- Personería Auxiliar (Gestión de Informática) deberá garantizar que la información que transita a través de la red cuenta con los protocolos de seguridad necesarios, asegurado su confidencialidad, disponibilidad e integridad.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 26  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá implementar la utilización de protocolos de seguridad para el cifrado de las claves.
- Personería Auxiliar (Gestión de Informática) deberá contar con protocolos de protección de los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la Entidad.


## 9.5. Control de accesos

La Personería de Medellín deberá reducir los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad estableciendo controles al acceso de redes, datos e información, además de la implementación de perímetros de seguridad para la protección de las instalaciones como las áreas de trabajo, los centros de datos, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado y otras áreas de trabajo externas o esenciales para el cumplimiento de las funciones misionales de la Entidad. El objetivo será controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad de la información (redes y sistemas/plataformas de información).

### 9.5.1. Política de control de accesos

La Personería de Medellín, deberá llevar a cabo el control de acceso a la información permitiendo mantener la trazabilidad de las acciones realizadas, identificando entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso y accesos denegados.

- Personería Auxiliar (Gestión de Informática) deberá establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Entidad.
- El acceso a la red de la Entidad estará controlado mediante un dispositivo de seguridad perimetral Firewall, que permite la separación de redes y el manejo de políticas de acceso a cada una de ellas. La modificación de estas reglas establecidas en el Firewall, deberán ser aprobadas por el personal responsable del Personería Auxiliar (Gestión de Informática) .
- Los funcionarios y contratistas que tengan acceso a la información misional no deberán realizar modificaciones sobre ella, sin la debida autorización, y deberán guardar la confidencialidad de la información a la cual tienen acceso.
- Está explícitamente prohibido transgredir los controles de seguridad establecidos por Personería

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 27  | de       | 65      |     |      |


Auxiliar (Gestión de Informática) ; la violación de esta política podrá acarrear consecuencias disciplinarias, civiles y penales según el caso.

- Personería Auxiliar (Gestión de Informática) deberá suministrar una herramienta para realizar conexiones remotas a la red de área local de la Entidad de manera segura para los funcionarios y contratistas que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.
- Personería Auxiliar (Gestión de Informática) deberá tener un procedimiento de creación de cuentas, donde estén definidas las condiciones de autorización y acuerdos de confidencialidad respectivos.
- Los funcionarios y contratistas deberán tener el Acuerdo de Confidencialidad firmado, otorgado por Personería Auxiliar (Gestión del Talento Humano) y la autorización de creación de cuentas otorgado por el jefe inmediato, para tener acceso lógico a los sistemas de información de la Entidad, según sea el caso.
- Los funcionarios, contratistas y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la Entidad deberán cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para las que fueron autorizados.

#### 9.5.2. Gestión de acceso de usuarios

La Personería de Medellín deberá garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios. Deberá controlar en todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información permitirá que no se realicen potenciales amenazas.

- Todos los usuarios de la Entidad tendrán un identificador de red único o ID del usuario, para su uso personal que permitirá validar los accesos y verificar su buen uso.
- Cada uno de los responsables de los activos de información deberá realizar revisiones periódicas de los derechos de acceso de los usuarios autorizados a los sistemas de información en intervalos establecidos con el fin de cancelar las cuentas redundantes o inactivas.
- La creación del registro de usuarios para otorgar y revocar el acceso a los sistemas de información, bases de datos y otros servicios deberá hacerse de acuerdo con el procedimiento establecido; para la creación o definición del usuario en red se debe seguir las siguientes especificaciones:
  - Primera letra del nombre.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 28  | de       | 65      |     |      |

- Primera letra del segundo nombre, de no tener segundo nombre se continuará con el siguiente ítem.
- Primer apellido.
- De coincidir con otro ID de usuario, se agrega la primera letra inicial del segundo apellido.
- Personería Auxiliar (Gestión de Informática) deberá asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos y/o equipos de la plataforma tecnológica, sean inhabilitados o eliminados cuando así se disponga.
- Personería Auxiliar (Gestión de Informática) deberá definir los lineamientos para las características que deben contener las contraseñas que se aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información. Lineamientos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- Personería Auxiliar (Gestión de Informática) deberá establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna.

### 9.5.3. Responsabilidades de los usuarios

La Personería de Medellín deberá garantizar que los usuarios entiendan que deben ser responsables de la protección de la información para su identificación. Los usuarios de los recursos tecnológicos y los sistemas de información deberán realizar un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

- Todos los usuarios serán responsables de las actuaciones realizadas con su usuario de red e identificación (usuario y contraseña) asignadas para el uso de los sistemas de información y demás recursos a los cuales se les proporcione acceso.
- Las contraseñas de red serán secretas y en ninguna circunstancia deberán ser compartidas o reveladas a otra persona.
- Los usuarios a los cuales se les otorgue acceso a la red de datos y comunicaciones, sistemas de información y demás servicios que hacen parte de la plataforma tecnológica de la Personería de Medellín deberán atender y acatar las políticas y directrices establecidas por la Entidad para la gestión de contraseñas.
- Los funcionarios, contratistas y terceros que tengan acceso a la información de la Personería de Medellín no deberán realizar modificaciones sobre la información sin la debida autorización,


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 29  | de       | 65      |     |      |

guardar la confidencialidad de la información a la cual tiene acceso y no vulnerar los controles de seguridad establecidos por el Personería Auxiliar (Gestión de Informática) .

- Personería Auxiliar (Gestión de Informática) deberá registrar todos los usuarios en la base de datos de usuarios y roles, y mantenerla actualizada.


#### 9.5.4. Control de Acceso a Sistemas de Información y Aplicaciones

- Todos los usuarios a quienes se les autorice el ingreso a los sistemas y aplicaciones deberán contar con un identificador único (usuario y contraseña), el cual será personal e intransferible.
- Ninguna persona recibirá credenciales de acceso a la plataforma tecnológica, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información e Informática vigente.
- El acceso a los sistemas de información y demás recursos de tecnología de la Personería de Medellín será autorizado por el funcionario responsable de su protección y salvaguarda. La Personería de Medellín deberá tener un procedimiento para gestionar el acceso a la información y sus sistemas de información.
- Las aplicaciones deberán garantizar que los usuarios puedan cambiar las contraseñas que les han sido asignadas la primera vez que ingresan a ella y con periodicidad cada 2 o 3 meses.
- Personería Auxiliar (Gestión de Informática) deberá asegurar la forma de identificar al usuario cuando solicita restablecer la contraseña por olvido o bloqueo, para lo cual asignará una contraseña temporal que debe ser cambiada por el usuario una vez ingrese al sistema.
- Si se sospecha que las contraseñas han sido empleadas por otras personas, se deben cambiar de inmediato.
- Las contraseñas no deben escribirse ni dejarse en lugares visibles a los demás usuarios o donde personas no autorizadas puedan tener acceso.
- Las contraseñas de administración de servicios (aplicaciones, bases de datos, dispositivos, servidores, controles de acceso, programas especiales y gestores, entre otros), deberán ser guardadas en documento digital, cifrado y con restricción de clave segura, que solamente podrá ser conocida por el Personería Auxiliar (Gestión de Informática) .
- Las contraseñas de administración deberán ser cambiadas cuando se haga uso de estas de manera regular y deberán cumplir con todos los demás requisitos generales de políticas de

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 30  | de       | 65      |     |      |

contraseñas establecidas.

- Las contraseñas establecidas deberán ser seguras, no repetidas en un periodo de tiempo o en cambios anteriores, deberán tener una longitud no menor a 8 caracteres y en lo posible no deberán contener palabras que se asocien a la vida personal de los usuarios (número de cédula, fechas de nacimiento, entre otros)
- Las cuentas de red se bloquearán después de tres (3) intentos fallidos con desbloqueo automático a los quince (15) minutos, además el sistema solicitará cambio de clave después de cumplido un periodo de tiempo de noventa (90) días calendario.
- Personería Auxiliar (Gestión de Informática) deberá asegurar que el número de sesiones concurrentes de un mismo usuario sea limitado.
- La eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red, los sistemas de información y bases de datos, de manera oportuna, cuando los funcionarios y contratistas se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo, se realizarán con las novedades enviadas al Personería Auxiliar (Gestión de Informática) por parte de Personería Auxiliar (Gestión del Talento Humano) en el formato establecido o por solicitud del jefe inmediato o supervisor del contrato por medio de la Personería Auxiliar (Gestión de Informática - Mesa de ayuda).
- La contraseña de administrador local de las estaciones de trabajo nunca caduca, esta contraseña es general para todas las estaciones de trabajo y se usará exclusivamente para efectos de soporte técnico por parte del equipo autorizado por Personería Auxiliar (Gestión de Informática) , en ninguna circunstancia esta contraseña será revelada a los usuarios no autorizados.
- Se prohibirá el uso de software o programas utilitarios que puedan violar o evadir los controles de seguridad para el acceso seguro a los sistemas y aplicaciones.
- Personería Auxiliar (Gestión de Informática) deberá implementar las medidas necesarias para limitar el acceso al código fuente de los sistemas de información y/o aplicativos de la Personería de Medellín.
- Solo se permitirá el acceso al código fuente de los sistemas de información y/o aplicativos de la Personería de Medellín al personal autorizado por el Personería Auxiliar (Gestión de Informática) .

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 31  | de       | 65      |     |      |


## 9.6. Cifrado

La Personería de Medellín asegurará el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información confidencial de la Entidad al momento de almacenarse o transmitirse. El objetivo es el de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas

- Personería Auxiliar (Gestión de Informática) deberá proporcionar los mecanismos o herramientas necesarias para cifrar la información confidencial de la Entidad, protegida por los propietarios de la información.
- Personería Auxiliar (Gestión de Informática) es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Personería de Medellín con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no rechazo en las comunicaciones o en el tratamiento de la información de la Entidad, adopta los controles de cifrado de datos que reduzcan los riesgos de seguridad de la información.
- El designado por Personería Auxiliar deberá declarar que sus funcionarios comprenden y aceptan la responsabilidad de custodia de las llaves de cifrado y las demás responsabilidades asociadas al rol.
- Personería Auxiliar (Gestión de Informática) suministrará las herramientas necesarias para garantizar el cifrado y envío seguro de la información confidencial, sensible, o reservada que será almacenada o transmitida al interior o exterior de la Entidad.
- Toda información sensible, confidencial o reservada que se transmita al interior o fuera de la Entidad debe ser encriptada y protegida con una contraseña segura, antes de enviarla al destinatario.
- La contraseña de encriptación deberá ser compartida con el destinatario por un medio diferente al del envío de la información.
- Personería Auxiliar (Gestión de Informática) deberá contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Consecuentemente se recomienda cifrar dicha información para mayor seguridad.

## 9.7. Seguridad Física y Ambiental


La Personería de Medellín deberá establecer perímetros de seguridad y áreas protegidas para facilitar

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 32  | de       | 65      |     |      |

la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la Entidad contra accesos físicos no autorizados. Además deberá controlar los factores ambientales de origen interno y externo para garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

### 9.7.1. Áreas seguras

- Todas las áreas designadas al procesamiento o almacenamiento de información sensible, además de aquellas en las que se encuentren los equipos de comunicaciones y seguridad perimetral y demás infraestructura de tecnologías de información, serán consideradas como áreas seguras y de acceso restringido para personal no autorizado por el Personería Auxiliar (Gestión de Informática).
- No se permite fumar, ni el ingreso o consumo de alimentos o bebidas en las instalaciones de centros de cómputo o de cableado.
- En las instalaciones donde se gestione, almacene y procesa información de la Personería de Medellín, deberán implementarse controles de acceso seguro, con el fin de prevenir accesos no autorizados, adulteración, pérdida, consulta, daños e interferencia en el funcionamiento de las aplicaciones, sistemas de información e información de la Entidad.
- Las puertas de acceso a las oficinas e instalaciones de la Personería de Medellín deberán permanecer cerradas y aseguradas, con el fin de prevenir el acceso de personal no autorizado.
- Personería Auxiliar (Gestión de Informática) deberá monitorear periódicamente la temperatura de los espacios destinados como centros de cómputo o cableado.
- Los funcionarios, contratistas y terceros deberán cumplir completamente con los controles físicos implantados por la Entidad, los ingresos y salidas a las instalaciones de la Entidad deben ser registrados.
- Todos los miembros de la Entidad y terceros deben portar el carné o tarjeta que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de la Entidad; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
- Los funcionarios, contratistas y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deberán velar por las condiciones físicas y medioambientales necesarias para certificar la protección y


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 33  | de       | 65      |     |      |

correcta operación de los recursos de la plataforma tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:

- Sistemas de control ambiental de temperatura y humedad
  - Sistemas de extinción de incendios
  - Sistemas de vigilancia y monitoreo
  - Alarmas en caso de detectarse condiciones ambientales inapropiadas.
- Personería Auxiliar (Gestión de Informática) deberá asegurar los recursos de la plataforma tecnológica, ubicados en las instalaciones que tienen bajo su custodia centros de cómputo y centros de cableado, se encuentren protegidos contra fallas o interrupciones eléctricas.
  - Personería Auxiliar (Gestión de Informática) deberá asegurar los recursos de la plataforma tecnológica, ubicados en las instalaciones que tienen bajo su custodia centros de cómputo y centros de cableado, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
  - Personería Auxiliar (Gestión de Informática) deberá asegurar los recursos de la plataforma tecnológica, ubicados en las instalaciones que tienen bajo su custodia centros de cómputo y centros de cableado, deberán asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.


### 9.7.2. Seguridad de los equipos

- La administración de hardware conectado a la red y la atención de nuevos requerimientos y adecuaciones debe realizarse de acuerdo con lo establecido en el procedimiento “Reporte, Solución y Análisis de Requerimientos” código PDPI033”; por ende no podrán conectarse computadores, servidores, dispositivos de comunicaciones como concentradores, switches, enrutadores o cualquier otro hardware a la red, sin la participación o supervisión de personal autorizado por el Personería Auxiliar (Gestión de Informática) .
- Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, seguridad en el suministro eléctrico y cableado y sistemas de detección y extinción de incendios.
- Se deberá prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de estos o deterioren la información almacenada en ellos. Se deberá evitar colocar encima o cerca de los computadores ganchos, clips, bebidas y comidas que se pueden caer

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 34  | de       | 65      |     |      |

accidentalmente dentro del equipo.

- El suministro de energía eléctrica deberá estar regulado a 110 voltios y con sistema de polo a tierra, salvo especificación contraria del fabricante o proveedor de los equipos y se deberá contar con sistema de energía ininterrumpida (UPS) y planta eléctrica para asegurar el apagado controlado y sistemático o la ejecución continua del ambiente tecnológico que sustenta las operaciones críticas de la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá elaborar el cronograma de mantenimiento preventivo, el cual será notificado a las dependencias con mínimo tres días hábiles de antelación con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos.
- Toda solicitud de mantenimiento correctivo o asistencia técnica deberá realizarse a través de la herramienta mesa de ayuda en la intranet, implementado por el Personería Auxiliar (Gestión de Informática) .
- Ningún funcionario o contratista diferente al personal autorizado por el Personería Auxiliar (Gestión de Informática) está autorizado para intervenir, efectuar reparaciones o modificaciones en los equipos de cómputo de la Entidad. El mantenimiento preventivo y correctivo debe ser realizado exclusivamente por personal especializado y autorizado por Personería Auxiliar (Gestión de Informática).
- Para trasladar o retirar equipos (incluidos la información y el software) por cambio del funcionario o contratista responsable o cambio en la ubicación del equipo deberá solicitarse al Personería Auxiliar (Gestión de Informática).
- Para el uso de un equipo fuera de la Entidad por parte de un funcionario o contratista deberá ser solicitado Personería Auxiliar (Gestión de Bienes Logísticos), quien autorizará mediante un oficio dirigido a la administración del edificio el retiro del dicho elemento.
- Cualquier cambio que se realice en el centro de datos o centros de cableado, y que potencialmente afecte los sistemas de información de la Entidad, deberá estar previamente autorizado y registrarse en una bitácora de ingreso al centro de datos.
- Toda persona que ingrese al centro de datos deberá estar autorizada y acompañada por un funcionario o contratista de Personería Auxiliar (Gestión de Informática). Los administradores del centro de datos mantendrán un registro de todas las visitas autorizadas a esta área, en el que se


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 35  | de       | 65      |     |      |

identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, actividad por la cual ingresaron y la persona que autorizó su ingreso. A su vez, todo equipo informático ingresado al centro de datos deberá ser registrado.

- Los funcionarios, contratistas y terceros no deberán mover o reubicar los equipos de cómputo pertenecientes a la Entidad, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de estos sin la autorización del Personería Auxiliar (Gestión de Informática) .
- Los funcionarios, contratistas y terceros no deberán consumir alimentos o ingerir líquidos mientras utilizan los equipos de cómputo.
- Personería Auxiliar (Gestión de Informática) deberá mantener los cables de red de los centros de datos claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Personería Auxiliar (Gestión de Informática) deberá contar con los planos que describan las conexiones del cableado.
- Personería Auxiliar (Gestión de Informática) deberá mantener el acceso a los centros de cableado solo para el personal autorizado.

### 9.7.3. Política de puesto de trabajo despejado y bloqueo de pantalla


- Los funcionarios y contratistas de la Entidad deberán conservar el escritorio del equipo, libre de información de uso interno o confidencial 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.
- Personería Auxiliar (Gestión de Informática) deberá aplicar un protector estándar en todas las estaciones de trabajo y equipos portátiles de la Entidad, de forma que se active luego de diez minutos sin uso. La pantalla de autenticación a la red de la Entidad deberá requerir solamente la identificación de la cuenta y una clave y no entregar otra información adicional y se configurará el ahorro de energía apagando la pantalla a los quince (15) minutos de inactividad
- Los funcionarios y contratistas deberán guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o de uso interno.
- Los funcionarios y contratistas no deberán dejar en el escritorio físico documentos de uso confidencial sin custodia.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 36  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de los puntos anteriores.
- Los funcionarios, contratistas y terceros de la Personería de Medellín deberán adoptar buenas prácticas para el manejo y administración de la información institucional física o digital que se encuentre a su cargo, con el fin de evitar que personas no autorizadas accedan a dicha información. Para ello, se deberá tener en cuenta lo siguiente:
- Cualquier funcionario o contratista que se ausente de su lugar de trabajo, deberá además de bloquear su estación de trabajo, guardar en un lugar seguro cualquier información que esté publicada en la intranet de la Personería de Medellín como documentos, medio magnético u óptico removible que contenga información confidencial.
- Si la estación de trabajo del personal está ubicada cerca de zonas de atención de público, al ausentarse de su lugar de trabajo deberá guardar también los documentos y medios que contengan información de uso interno.
- Al finalizar la jornada de trabajo, el personal deberá apagar su equipo de cómputo, guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los sistemas de información y servidores.
- El papel tapiz se configurará automáticamente en cada uno de los equipos conectados a la red de la Personería de Medellín, éste sirve para difundir información institucional y debe ser remitido por la oficina Asesora de Comunicaciones.
- Al imprimir información confidencial, reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.
- Los archivos digitales que contengan información sensible o confidencial de la Personería de Medellín deberán ser almacenados en rutas que impidan el fácil acceso por terceros, y no se deberán guardar en el área de escritorio de la pantalla del computador.

### 9.8. Seguridad de las Operaciones

La Personería de Medellín deberá asegurar las operaciones correctas y seguras de los servicios de procesamiento de información. Además deberá crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de operación. Adoptará medidas de seguridad encaminadas a prevenir la proliferación y expansión de


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 37  | de       | 65      |     |      |

software malicioso que son catalogadas como amenazas en potencia y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques.

### 9.8.1. Responsabilidades y procedimientos de operación

La Personería de Medellín deberá evitar el acceso físico no autorizado, los daños e interferencias a la información de la Entidad y las instalaciones de procesamiento de la información.

- La Entidad establecerá procedimientos relacionados con la operación y administración de la información institucional, estarán documentados y serán puestos a disposición del personal que lo requiera.
- Personería Auxiliar (Gestión de Informática) deberá mantener y proveer a su personal, los manuales, guías y procedimientos de configuración de equipos, plataformas informáticas y demás servicios de tecnologías de información.
- Los ambientes de desarrollo, prueba y producción estarán separados físicamente (diferente hardware) siempre que sea posible, y se definirán y documentarán las reglas para la transferencia de software desde el estado de prueba hacia el estado producción.
- Personería Auxiliar (Gestión de Informática) cuenta con el procedimiento “Procedimiento de Gestión de Cambios” para el control de cambios en el desarrollo de nuevas aplicaciones y en los diferentes ambientes y en general para cualquier cambio que afecte los servicios y la infraestructura
- Personería Auxiliar (Gestión de Informática) deberá garantizar que todo cambio realizado a un componente de la plataforma tecnológica, los cuales generen modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes no afecta la correcta operación de esta ni de otros servicios.
- Personería Auxiliar (Gestión de Informática) deberá garantizar que todo cambio realizado sobre la plataforma tecnológica de la Entidad quedará formalmente documentado desde su solicitud hasta su implementación.
- Los responsables de los activos de información tecnológicos y recursos informáticos deberán solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.
- Personería Auxiliar (Gestión de Informática) como administradores de los activos de información

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 38  | de       | 65      |     |      |


tecnológicos y recursos informáticos, deberán garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios.

- Personería Auxiliar (Gestión de Informática) deberá supervisar continuamente el uso de los recursos con el fin de realizar los pertinentes ajustes, revisar las proyecciones para las futuras necesidades de capacidad y asegurar el rendimiento del sistema requerido.
- Personería Auxiliar (Gestión de Informática) deberá realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Aspectos por considerar:
  - Consumo de recursos de procesadores, memorias, discos.
  - Servicios de impresión
  - Ancho de banda, internet y tráfico de las redes de datos.

#### 9.8.2. Protección contra Códigos Maliciosos

La Personería de Medellín proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de procesamiento de está adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la incidencia de software malicioso. Además proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios frente a los ataques. Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.


- Todos los equipos de cómputo de propiedad de la Entidad deberán tener instalado el software de antivirus debidamente actualizado y licenciado a nombre de la Personería de Medellín. Así que todo equipo nuevo deberá ser incluido dentro del dominio de la red, para que apliquen las actualizaciones y detecciones correspondientes.
- Los funcionarios, contratistas y terceros deberán contar con un antivirus actualizado en sus dispositivos personales tales como: portátiles o celulares, si desean ingresar a la red de datos de la Entidad.
- Antes de distribuir, archivos a otros usuarios internos o externos en los equipos de cómputo de la Entidad, se deberá hacer un análisis de los archivos y medios con el software de antivirus.
- Estará prohibido desinstalar o deshabilitar el software antivirus de los computadores de la Entidad por parte de los usuarios. Si existen indicios de infección por virus informáticos, se debe realizar un análisis del equipo y sus archivos y verificar su eliminación mediante el software de antivirus y reportar el incidente a el Personería Auxiliar (Gestión de Informática) .

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 39  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenido y administrada en la plataforma tecnológica de la Entidad y los servicio que se ejecutan en está.
- Personería Auxiliar (Gestión de Informática) deberá garantizar que el software antivirus, antimalware, antispam, antispyware cuente con las licencias de uso, garantizando su autenticidad y su posibilidad de actualización periódica frente a las últimas bases de datos del proveedor del servicio.
- Personería Auxiliar (Gestión de Informática) deberá garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- Todo medio de almacenamiento removible como discos duros externos, dispositivos USB, discos compactos, entre otros que vaya a ser conectado a un equipo de la Entidad, debe ser analizado con el software de antivirus instalado por el Personería Auxiliar (Gestión de Informática) en los equipos de cómputo de la Entidad.
- Estará prohibido el uso e instalación de software no autorizado por el Personería Auxiliar (Gestión de Informática) . En caso de necesitar la instalación de algún software, el funcionario o contratista responsable debe solicitar la autorización y apoyo a el Personería Auxiliar (Gestión de Informática) .
- Personería Auxiliar (Gestión de Informática) estará facultada para revisar periódicamente la información y el software instalado en los equipos de cómputo de la Personería de Medellín y realizará la eliminación de los archivos o información no autorizados que puedan atentar contra la seguridad de la información, así como la desinstalación inmediata del software no autorizado.
- Ningún funcionario, contratista o tercero deberá descargar software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Personería Auxiliar (Gestión de Informática) .
- Los funcionarios, contratistas o tercero no deberán realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Outlook, Office, navegadores u otros programas, para detectar y prevenir la propagación de virus.


### 9.8.3. Copias de seguridad

La Personería de Medellín garantizará la generación de copias de respaldo y almacenamiento de su

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 40  | de       | 65      |     |      |

información crítica, con el propósito de proteger la información de la Entidad, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de copias de respaldo. Se considera como información para ser respaldada aquella que es exclusivamente de carácter institucional.

- Personería Auxiliar (Gestión de Informática) será la responsable de realizar copias de respaldo de los datos que hacen parte de los sistemas de información y software de aplicaciones, bases de datos de servidores físicos y virtuales, y carpetas compartidas, que sean administrados por el Personería Auxiliar (Gestión de Informática) y que se encuentran alojados en el centro de datos de la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá determinar los roles de usuario, según su responsabilidad y tareas asignadas dentro de la Entidad, que intervienen dentro del proceso de backup:
  - Administrador de backup: persona encargada de realizar los backup.
  - Transportador: encargado de llevar los backup fuera de las instalaciones de la Entidad.
  - Probador: Encargado de probar backup cada cierto período de tiempo.
- Personería Auxiliar (Gestión de Informática) deberá programar y realizar pruebas de restauración periódicas de la información contenida en las copias de respaldo para comprobar su correcto funcionamiento.
- Las copias de respaldo realizadas por el Personería Auxiliar (Gestión de Informática) deberán ser almacenadas de forma segura para garantizar que no sean manipuladas por personas no autorizadas y sean almacenados en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.
- Personería Auxiliar (Gestión de Informática) deberá llevar un registro de las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de estas que contenga datos como fecha del respaldo, restauraciones realizadas, ubicación de medios, entre otros
- Al cumplir el ciclo de vida útil, los medios de almacenamiento de las copias de respaldo serán desechadas de forma segura, evitando la recuperación de la información contenida y el acceso por parte de personas no autorizadas.
- La información corporativa deberá residir en las bases de datos de los servidores o en las unidades lógicas destinadas para ello, si por alguna razón esto no es posible y su manejo se

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 41  | de       | 65      |     |      |


realiza en forma local, el usuario deberá documentar los desarrollos realizados y posterior almacenamiento de esta tanto en los servidores como en las bases de datos. Personería Auxiliar (Gestión de Informática) no se hace responsable por la información almacenada en forma local. Por tanto la custodia y respaldo de la información que se almacene en los equipos de cómputo localmente será de responsabilidad de cada funcionario o contratista dueño o generador de dicha información.

- Personería Auxiliar (Gestión de Informática) deberá verificar la integridad de los backup que se están almacenando, de acuerdo con el procedimiento de revisión periódica, con el fin de asegurar que al momento de requerir restaurar alguno de ellos funcione como se espera.
- Los directores o jefes de área deberán identificar la información que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

#### 9.8.4. Registro de actividad y supervisión

La Personería de Medellín realizará monitoreo permanente del uso que dan los funcionarios y contratistas a los recursos de la plataforma tecnológica y los sistemas de información de la institución. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos.

- Personería Auxiliar (Gestión de Informática) en conjunto con los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la Entidad.
- La oficina de Control Interno y designado por Personería Auxiliar deberán determinar los periodos de retención de archivos de auditoría y los eventos a auditar en los recursos tecnológicos y los sistemas de información de la Entidad, con base en las tablas de retención documental.
- Personería Auxiliar (Gestión de Informática) deberá determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- Personería Auxiliar (Gestión de Informática) deberá habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- Personería Auxiliar (Gestión de Informática) deberá certificar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información. Estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 42  | de       | 65      |     |      |

- Todas las aplicaciones en producción que la Entidad valore pertinentes y que contengan información misional de la Personería de Medellín deberán generar logs o trazas de auditoría; igualmente los sistemas que operen y administren información misional valiosa o crítica para la Entidad, deberán contener archivos de logs que contengan evidencia sobre los eventos relevantes que sucedan con la información, y con la seguridad necesaria para su consulta, modificación o borrado.
- Todos los logs del sistema y de las aplicaciones deberán mantenerse en forma segura, de tal forma que se evite el acceso no autorizado para garantizar la seguridad de esta información.
- La oficina de Control Interno deberá revisar periódicamente los archivos de auditoría de la plataforma tecnológica y los sistemas de información para identificar brechas de seguridad y otras actividades propias del monitoreo.
- La adquisición de nuevo software debe garantizar el registro de logs de auditoría de las actividades realizadas por los usuarios y administradores en los sistemas de información intervenidos. Se deberá usar controles de integridad sobre estos registros.
- En los aplicativos existentes y en los nuevos desarrollos se deberán registrar en los logs de auditoría eventos como transacciones sobre datos, fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, fallas en los módulos criptográficos, entre otros.

#### 9.8.5. Control del software en explotación

La Personería de Medellín a través del Personería Auxiliar (Gestión de Informática) designará responsables y establecerá procedimientos para controlar la instalación de software operativo, garantizará el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

- Personería Auxiliar (Gestión de Informática) deberá establecer responsabilidades y procedimientos para controlar la instalación de software en los sistemas operativos, que interactúen con los procedimientos de control de cambios existentes en la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá garantizar que el software operativo instalado en la plataforma tecnológica de la Entidad tenga soporte de los proveedores.
- Personería Auxiliar (Gestión de Informática) deberá otorgar accesos temporales y controlados a

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 43  | de       | 65      |     |      |


los proveedores para realizar las actualizaciones sobre el software operativo, y también monitorear dichas actualizaciones.

- Personería Auxiliar (Gestión de Informática) deberán validar los riesgos que genera la migración hacia nuevas versiones de los softwares operativos. Se deberá garantizar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- Personería Auxiliar (Gestión de Informática) deberá implementar los controles necesarios para evitar la instalación de software en los equipos de cómputo de la Entidad.
- Personería Auxiliar (Gestión de Informática) validará y realizará las pruebas calidad y funcionamiento del software a instalar, antes de ser puesto en producción.
- Personería Auxiliar (Gestión de Informática) será la responsable de analizar el software y autorizar su instalación, el cual debe ser realizado exclusivamente por personal competente y autorizado.
- Personería Auxiliar (Gestión de Informática) deberá mantener un registro actualizado del software propiedad de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) deberá establecer responsabilidades y procedimientos para controlar la instalación del software en los equipos de cómputo.
- Personería Auxiliar (Gestión de Informática) deberá asegurarse que tanto las aplicaciones desarrolladas localmente como las de terceros, realicen las respectivas pruebas antes de salir a producción.

#### 9.8.6. Gestión de Vulnerabilidad Técnica

Personería Auxiliar (Gestión de Informática) de la Personería de Medellín revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica a través de la realización de pruebas, con el objeto de realizar la corrección sobre los hallazgos obtenidos por estas pruebas.

- Personería Auxiliar (Gestión de Informática) deberá revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y deberá reportarlas a los administradores de la plataforma tecnológica con el fin de prevenir la exposición al riesgo de estos. En caso de ser necesario, las revisiones podrán realizarse mediante la contratación de una asistencia técnica especializada. El resultado de las revisiones se presentará en un informe técnico para su interpretación y remediación por parte de los especialistas de la Entidad.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 44  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá realizar o contratar a terceros para la realización de pruebas de vulnerabilidades, escaneos de sistemas y hacking ético en ciclos establecidos, que cumplan con estándares internacionales.
- Personería Auxiliar (Gestión de Informática) deberá generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- Personería Auxiliar (Gestión de Informática) deberá generar los lineamientos y estándares a seguir para la configuración segura de la plataforma tecnológica.
- Personería Auxiliar (Gestión de Informática) deberá establecer las restricciones y limitaciones para la instalación de software en los equipos de cómputo de la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá configurar los recursos de la plataforma tecnológica siguiendo los lineamientos y estándares de configuración segura establecidos.


### 9.9. Seguridad en las Telecomunicaciones

La Personería de Medellín proveerá a través del Personería Auxiliar (Gestión de Informática) los mecanismos de control necesarios para garantizar la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo velará por tener los mecanismos de seguridad que protejan la integridad y la confidencialidad de a la información que se transporta a través de dichas redes de datos.

#### 9.9.1. Gestión de la seguridad en las redes

La Personería de Medellín deberá evitar el acceso físico no autorizado, los daños e interferencias a la información de la Entidad y las instalaciones de procesamiento de la información.

- Personería Auxiliar (Gestión de Informática) deberá adoptar medidas para garantizar la disponibilidad de los recursos y servicios de red de la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- Personería Auxiliar (Gestión de Informática) deberá mantener las redes de datos segmentadas por dominios, grupos de servicio, grupos de usuarios, ubicación geográfica o cualquier clasificación que considere conveniente.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 45  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá gestionar y establecer mecanismos y controles para prestar el servicio de redes de datos y comunicaciones en la Entidad y encaminado por la protección de los datos y los servicios conectados en las redes de la Personería de Medellín contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:
  - Establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.
  - Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
  - Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- Personería Auxiliar (Gestión de Informática) deberá garantizar la confidencialidad de las políticas de enrutamiento y direccionamiento de las redes de datos y comunicaciones de la Entidad.
- Las direcciones IP internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la Entidad, serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la Entidad sin la previa autorización del Personería Auxiliar (Gestión de Informática) .
- Personería Auxiliar (Gestión de Informática) deberá garantizar que los equipos de acceso a la red estén protegidos contra accesos no autorizados.
- Los funcionarios, contratistas o terceros que desarrollen actividades en los sistemas de información de la Entidad de manera remota, deberán utilizar equipos de cómputo seguros que garanticen la no afectación de la seguridad de la red.
- La Personería de Medellín implementará mecanismos de segmentación de redes a través de LAN virtuales, dependiendo de la complejidad de los recursos y servicios involucrados, con el fin de contribuir al control de acceso y optimizar el rendimiento en la red.

### 9.9.2. Políticas y procedimientos de transferencia de información

La Personería de Medellín establecerá mecanismos seguros para la transferencia de información institucional internamente y con terceros, en cumplimiento de sus funciones y obligaciones legales.


- La transferencia de la información institucional de la Personería de Medellín se controlará según los niveles de clasificación legal de la información determinados y las políticas de seguridad de la información de la Entidad. En caso de que se requiera intercambiar información sensible, reservada, confidencial o pública clasificada, se deberán implementar los controles de cifrado de información de acuerdo con lo establecido en la política de controles criptográficos.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 46  | de       | 65      |     |      |


- Los intercambios de información con terceros deberán estar soportados mediante contratos o acuerdos debidamente formalizados, estableciendo los medios y controles para el tratamiento de la información. También se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encargadas.
- La Personería de Medellín proporcionará tecnologías de acceso remoto a sus funcionarios y contratistas a través de medios como VPN (Red virtual privada), y autorizará su uso de forma particular cuando así se requiera. Personería Auxiliar (Gestión de Informática) garantizará un adecuado modelo de seguridad.
- Todos los computadores de la Entidad que sean accedidos remotamente a través de mecanismos como Internet, enlaces dedicados y otros, deberán ser protegidos por mecanismos de control de acceso aprobados por el Personería Auxiliar (Gestión de Informática).
- Como requisito para interconectar las redes de la Personería de Medellín con otras redes externas, los sistemas de comunicación de terceros deberán cumplir con los requisitos de seguridad dispuestos por este documento.
- La Personería de Medellín se reservará el derecho de cancelar o terminar la conexión a sistemas de terceros, que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos o acordados.
- Para la transmisión o envío interno o externo de información sensible, confidencial o reservada, a través de medios electrónicos, incluido el correo institucional, se deberá asegurar de aplicar las medidas de seguridad necesarias y como mínimo, cumplir con el numeral "Políticas de Cifrado" establecidas en el presente manual.
- No estará permitido el envío de información institucional sensible, clasificada o reservada a través de plataformas gratuitas como (Wetransfer, Google Drive, Droopbox, WhatsApp, Messenger, entre otros), sin previa autorización.

### 9.9.3. Políticas y procedimientos de uso del correo electrónico


La Personería de Medellín entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios, contratistas y terceros, proporcionará y garantizará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 47  | de       | 65      |     |      |

- Todo funcionario o contratista inscrito en la Personería de Medellín dispondrá de una cuenta de correo electrónico activa, y para su creación se debe seguir con el procedimiento “PDPI031 Procedimiento de Gestión de Usuarios y Contraseñas” establecido de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) deberá generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- No está permitido almacenar información institucional sensible, clasificada o reservada en la nube que no esté autorizada.
- El servicio de correo electrónico institucional deberá ser usado exclusivamente para las tareas propias de la función desarrollada por la Personería de Medellín.
- El servicio de correo electrónico oficial de la Personería de Medellín será el aprobado por el Personería Auxiliar (Gestión de Informática) .
- Personería Auxiliar (Gestión de Informática) deberá asegurar que los mensajes electrónicos están protegidos contra código malicioso y pudiera ser transmitido a través de estos.
- Personería Auxiliar (Gestión de Informática) deberá generar campañas de concientización a todos sus usuarios respecto a las precauciones que deben adoptar en el intercambio de información confidencial y de uso interno por medio del correo electrónico.
- Los funcionarios, contratistas y terceros deberán reconocer y aceptar que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su responsabilidad.
- La vigencia de la cuenta para funcionarios y contratistas comprende el periodo desde la fecha de ingreso o firma del contrato y finaliza el último día de la fecha de retiro o terminación o suspensión del contrato.
- Está prohibido utilizar el correo electrónico personal, para el envío y recepción de información institucional sensible, clasificada o reservada.
- La clave de acceso al servicio de correo electrónico es personal e intransferible, no deberá ser divulgada a ninguna persona y para su gestión se deberá seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información - SGSI de la Personería de Medellín.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 48  | de       | 65      |     |      |

- Las contraseñas de las cuentas de correo institucional genéricas o que no estén asociadas a un usuario particular (por ejemplo info@personeriamedellin.gov.co), deberán ser cambiadas cuando la persona encargada de administrarla sea retirada de la Entidad o trasladada de dependencia.
- La Personería de Medellín podrá supervisar el uso del servicio de correo electrónico para verificar que se está usando para el cumplimiento de las funciones misionales de la Entidad, en los procesos de verificación de uso apropiado del servicio de correo electrónico se respetará el derecho a la privacidad e intimidad del titular de la cuenta de correo electrónico.
- En los casos en los que se requiera envío o recepción de información confidencial, sensible, reservada o pública clasificada, el usuario del servicio de correo electrónico deberá cumplir con las políticas de cifrado y criptografía establecidas por la Entidad, y si es el caso solicitar apoyo técnico a el Personería Auxiliar (Gestión de Informática) .
- El uso de la cuenta de correo será con fines del cumplimiento de las funciones u objeto contractual y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los funcionarios y contratistas de la Entidad.
- Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.
- Es responsabilidad del funcionario o contratista depurar su cuenta periódicamente como el único responsable de realizar las copias de seguridad de sus correos.
- El usuario deberá leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.
- Solo podrán enviar correos masivos aquellas dependencias que por su naturaleza de socialización y sensibilización lo requieran a través de la cuenta de correo del jefe de la dependencia.
- El incumplimiento por parte del funcionario y contratista de los requerimientos o el mal manejo de su cuenta de correo institucional, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la oficina de Gestión del Talento Humano para que proceda disciplinariamente.
- No están autorizados los siguientes usos del servicio de correo electrónico y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:
  - Exceder los servicios para los cuales se autorizó la cuenta.
  - Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 49  | de       | 65      |     |      |

identificar plenamente a su autor o autores o enviar anónimos.

- Difundir “cadenas” de mensajes que saturen el servicio entre otros problemas.
  - Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.
  - Agredir o lesionar directa o indirectamente a otras personas a través del envío de mensajes con contenido que atente contra la integridad y el buen nombre de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Entidad o esté
  - Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
  - Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
  - Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales o afines a la misión institucional.
  - Enviar correos de información masivos sin estar autorizado para ello.
  - Envío de mensajes no deseados o que puedan ser considerados como SPAM.
- Para reducir el riesgo de los virus, no abra correos de destinatarios desconocidos y/o que no hacen referencia al asunto.
  - No está permitido reenviar correos basura o SPAM, estos correos son fácilmente identificables ya que incitan al usuario a enviar cientos de correos a diferentes destinatarios, con la promesa de que esto les mejorará la vida.
  - Los correos que entran y salen por Internet, no pueden exceder del tamaño definido en los lineamientos del Departamento de Informática , para evitar que el desempeño del canal de conexión a Internet se vea afectado.
  - La información contenida en el correo electrónico debe ser depurada periódicamente, solo se debe almacenar información de carácter institucional, las fotos, música y videos personales no deben permanecer almacenadas en el buzón; de ser detectas serán eliminadas por el Departamento de Informática .
  - Se permite el uso del correo electrónico siempre y cuando se haga de manera responsable y no provoque problemas legales a la Entidad; no se utilice para fines lucrativos personales; no contravenga las políticas y directrices de la Entidad; no atente contra la imagen de la Entidad; y no interfiera con el trabajo de los funcionarios.
  - Como norma general está prohibido enviar mensajes de manera masiva; cadenas de cartas, falsos virus entre otros, excepto si los mensajes contienen información de interés institucional, en cuyo caso se utilizará la plantilla de Comunicación interna y se seleccionará el grupo de Usuarios

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 50  | de       | 65      |     |      |


destinatarios del mensaje.

- Están autorizados para el envío de mensajes electrónicos masivos los funcionarios del nivel Directivo, y los administradores de correo electrónico, de red del Personería Auxiliar (Gestión de Informática) , oficina Asesora de Comunicaciones y Gestión del Talento Humano. Los demás funcionarios deberán solicitar la autorización del Personero Auxiliar.
- Las cuentas de los funcionarios y/o contratistas que se retiren de la entidad se desactivarán y eliminarán después de veinte (20) días de su desvinculación, previa comunicación al Personería Auxiliar (Gestión de Informática) por medio de la mesa de ayuda.
- Los correos electrónicos de los buzones de algunos funcionarios y/o contratistas que se retiren se realizara el backup correspondiente para futuras consultas. Estos buzones estarán almacenados por un término de 4 años, previa comunicación al Personería Auxiliar (Gestión de Informática) .
- Los archivos y carpetas de las unidades de red compartidas de los funcionarios, colaboradores y/o contratistas se almacenará en las unidades lógicas destinadas para el almacenamiento. Sera eliminados permanentemente al pasar 4 años solo permanecerán históricamente los archivos y carpetas de Personero Delegados 20 D, 17D, jefes de proceso y coordinadores.
- Al momento de enviar y responder un correo electrónico el sistema de correo insertará de forma automática la información del funcionario (Nombre Completo, Cargo, Área, Dirección, teléfono, extensión e Email).
- El correo electrónico debe utilizarse de forma responsable; su principal fin es servir como herramienta para agilizar las comunicaciones oficiales que apoyen la gestión institucional. Se debe utilizar la administración, operación y uso del correo electrónico como un instrumento de comunicación organizacional para facilitar el intercambio de información de los funcionarios de la Personería de Medellín.


#### 9.9.4. Política de uso adecuado de internet

La Personería de Medellín consecuente de la importancia de internet como una herramienta para el desempeño de las labores, proporcionará los recursos necesarios para garantizar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias de la Entidad.

- Personería Auxiliar (Gestión de Informática) deberá proporcionar los recursos necesarios para la implementación, mantenimiento y administración necesarios para prestación segura del servicio de internet, bajo las restricciones de los perfiles establecidos.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 51  | de       | 65      |     |      |

- Personería Auxiliar (Gestión de Informática) deberá diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.
- Personería Auxiliar (Gestión de Informática) deberá monitorear continuamente los canales del servicio de internet, en cuanto a carga y tráfico.
- Personería Auxiliar (Gestión de Informática) deberá implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios restringidos.
- Personería Auxiliar (Gestión de Informática) deberá generar registros correspondientes con la navegación y acceso de los usuarios a internet y establecerá procedimientos de monitoreo sobre el uso del servicio de internet.
- El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Personería de Medellín los usos diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio.
- Personería Auxiliar (Gestión de Informática) establecerá canales dedicados para los sistemas de información para optimizar su rendimiento.
- Todos los funcionarios y contratistas que en el desarrollo de sus funciones utilicen el servicio de acceso internet serán responsables del cumplimiento de las políticas de seguridad de la información de Entidad.
- Todo usuario será responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de la Personería de Medellín o descargue desde internet empleando la cuenta de acceso que se le ha suministrado.
- La Personería de Medellín podrá supervisar el acceso del servicio de internet para certificar que se está usando para el cumplimiento de las funciones institucionales, en los procesos de verificación del uso apropiado del servicio de acceso a Internet se respetan el derecho a la intimidad y privacidad del titular de la cuenta de acceso.
- El acceso a Internet deberá ser autorizado por la Personero Auxiliar, o por quien deleguen.
- Se les suspenderá el servicio de Internet a los usuarios que tengan un reporte de navegación alto


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 52  | de       | 65      |     |      |

y que las páginas visitadas no sean de carácter institucional.

- La Personería restringirá a los usuarios descargar archivos que pongan en riesgo las seguridades de la red de datos y el desempeño del canal de comunicaciones con Internet, estos archivos son: Música (\*.mp3), Videos (\*.mpg, \*.avi, \*.flv), .EXE, .COM, .DAT, .PIF, entre otros Si el archivo que se trata de descargar se encuentra en esta lista, la conexión es rechazada indicando que por política institucional este acceso está restringido.

Para el caso en que sea absolutamente necesario la descarga de un archivo de tipo restringido, se debe solicitar al Departamento de Informática para que se programe la descarga a una hora en que no se sature el canal de Internet que la Personería posee.

- No estarán autorizados los siguientes usos del servicio de acceso a internet y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:
  - Descargar o distribuir archivos con virus, gusanos, troyanos o la trasmisión de archivos de imagen, sonido y video que no sean de tipo institucional.
  - Acceder, descargar o transmitir información sometida a derechos de autor cuando no se tienen los derechos respectivos (juegos, música, videos, obras literarias, pictóricas, imágenes, entre otros).
  - Descargar archivos o instalar programas de sitios web desconocidos o gratuitos sin previa autorización del Personería Auxiliar (Gestión de Informática) .
  - El acceso a sitios de música, juegos u otros sitios de entretenimiento online.
  - El acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos aquellos que hacen parte de la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
  - El acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo en los casos que estén debidamente autorizados en cumplimiento de las funciones, caso particular de investigaciones en procesos disciplinarios o administrativos; en tal caso se deben gestionar los mecanismos de acceso seguro en canales protegidos y configurados por personal autorizado por el Personería Auxiliar (Gestión de Informática) .
  - Acceder a sitios web de carácter discriminatorio, racista o material potencialmente ofensivo para las personas, incluyendo, bromas de mal gusto, prejuicios, menosprecio o acoso.
  - Acceder a sitios de hacking o sitios reconocidos como inseguros para la seguridad de la información, los cuales puedan poner en riesgo la integridad, disponibilidad y confidencialidad de la información de la Personería de Medellín salvo en los casos que se requiera para el cumplimiento de las funciones, en cuyo caso se deben gestionar los mecanismos de acceso seguro en canales protegidos y configurados por personal autorizado por el Personería Auxiliar (Gestión de Informática) .


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 53  | de       | 65      |     |      |

## 9.10. Adquisición, Desarrollo y Mantenimiento de Sistemas

La Personería de Medellín asegurará que el software adquirido o desarrollado al interior como por terceros, cumplirá con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información y el Personería Auxiliar (Gestión de Informática) incluirán necesidades de seguridad en la definición de requerimientos y luego se asegurarán de que estos hayan sido atendidos durante las pruebas realizadas sobre los desarrollos del software construido.

### 9.10.1. Establecimiento de los requisitos de seguridad de los sistemas de información

- Personería Auxiliar (Gestión de Informática) deberá establecer una metodología para el desarrollo de software, que incluya la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, para proporcionar a los terceros proveedores un enfoque claro de lo que se espera, incluido dentro de la arquitectura, seguridad, hardware y software.
- Todos los sistemas de información o desarrollos de software deberán tener un área propietaria dentro de la Entidad, formalmente asignada.
- Personería Auxiliar (Gestión de Informática) deberá incluir en la definición de requerimientos de seguridad de los sistemas de información o desarrollos, aspectos como la estandarización herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
- Los terceros proveedores o desarrolladores de sistemas de información deberán documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada desarrollo, de acuerdo con los parámetros de seguridad y los controles deseados, y a las disposiciones del presente manual.
- Los terceros proveedores o desarrolladores de sistemas de información deberán garantizar que todo el sistema de información o desarrollo adquirido o construido a la medida, debe usar herramientas de desarrollo licenciadas, vigentes y reconocidas en el mercado, condiciones de uso y derechos de propiedad intelectual.
- Los terceros proveedores o desarrolladores de sistemas de información deberán deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los terceros proveedores o desarrolladores de sistemas de información deberán establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez cumpla esta tiempo.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 54  | de       | 65      |     |      |

- Los terceros proveedores o desarrolladores de sistemas de información deberán garantizar que no se permitan conexiones recurrentes a los sistemas de información con el mismo usuario.
- La redacción de cada uno de los contenidos de los portales wweb e intranet de la Personería de Medellín estará a cargo de los gestores de contenido asignados por cada dependencia y deberá producirse conforme a los requisitos establecidos con anterioridad.
- Los terceros proveedores o desarrolladores que implemente un sistema de información deberán proporcionar los respectivos manuales:
  - Manual del usuario que describa los procedimientos de operación.
  - Manual técnico que describa su estructura interna, programas, catálogos y archivos.

#### 9.10.2. Seguridad en los procesos de desarrollo y soporte


Para el desarrollo de software al interior de la Personería de Medellín se deberá realizar un proceso de planificación de los desarrollos en donde se determine la respectiva metodología a usar, las etapas de desarrollo, la estructura de componentes a elaborar, los responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad, teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de la Entidad. Las etapas de desarrollo deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.

- Los propietarios de los sistemas de información, junto al Personería Auxiliar (Gestión de Informática) serán responsables de realizar las pruebas para asegurar que éstos cumplen con los requisitos de seguridad establecidos antes del paso a producción, usando una metodología establecida para este fin, documentando las pruebas realizadas y aprobando los pasos a producción.
- Personería Auxiliar (Gestión de Informática) deberá implantar los controles necesarios para garantizar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- Personería Auxiliar (Gestión de Informática) deberá contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad.
- Personería Auxiliar (Gestión de Informática) deberá asegurarse que los sistemas de información adquiridos o desarrollados por terceros, cuente con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- Personería Auxiliar (Gestión de Informática) deberá generar una metodología de pruebas al

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 55  | de       | 65      |     |      |

software desarrollado que contenga pautas para la selección de escenarios, niveles, tipo, datos de prueba sugerencias de documentación.


- Personería Auxiliar (Gestión de Informática) deberá asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que están ejecutando la última versión aprobada del sistema.
- Los terceros proveedores de sistemas de información deberán considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida, pasando desde el diseño hasta la puesta en marcha.
- Personería Auxiliar (Gestión de Informática) velará porque se mantenga un nivel adecuado de soporte para garantizar la solución de problemas que se presenten en el software; este soporte debe contemplar aspectos como tiempos de respuesta aceptables, considerados en los Acuerdos de Niveles de Servicio.
- Los terceros proveedores o desarrolladores de sistemas de información deberán garantizar que los sistemas construidos validen la información dada por los usuarios antes de procesarla, teniendo en cuenta aspectos como; tipos de datos, rangos validos, longitud, lista de caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los terceros proveedores o desarrolladores de sistemas de información deberán garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponible en todas las páginas protegidas por autenticación.
- En los procesos de desarrollo el Personería Auxiliar (Gestión de Informática) se asegurará de establecer las condiciones necesarias para la transferencia de los derechos de propiedad intelectual de códigos fuentes.
- Los terceros proveedores o desarrolladores deberán proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en los sistemas de información o aplicativos; deberá contemplar tiempos de respuesta aceptables.
- Los terceros proveedores o desarrolladores deberán construir los sistemas de información o aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 56  | de       | 65      |     |      |

- Los terceros proveedores o desarrolladores deberán asegurar el manejo de operaciones sensibles o críticas en los sistemas de información o aplicativos desarrollados permitiendo el uso de dispositivos adicionales como parámetros adicionales de verificación.
- Los terceros proveedores o desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.
- Los terceros proveedores o desarrolladores deberán garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; también deben implementar mensajes de error genéricos.
- Los terceros proveedores o desarrolladores deberán remover todas las funcionalidades y archivos que no sean necesarios para los sistemas de información o aplicativos, previo a la puesta en producción.
- Los terceros proveedores o desarrolladores deberán prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los terceros proveedores o desarrolladores deberán evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los terceros proveedores o desarrolladores deberán implementar los controles necesarios para la transferencia de archivos, como:
  - Exigir autenticación
  - Vigilar los tipos de archivos a transmitir
  - Almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
  - Eliminar privilegios de ejecución a los archivos transferidos
  - Asegurar que dichos archivos sólo tengan privilegios de lectura.
- Los terceros proveedores o desarrolladores deberán proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los terceros proveedores o desarrolladores deberán asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

### 9.10.3. Datos de prueba

Personería Auxiliar (Gestión de Informática) de la Personería de Medellín entregará los datos de

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 57  | de       | 65      |     |      |

prueba a los terceros proveedores o desarrolladores de sistemas de información, garantizando que no corresponden a información real de los ambientes de producción.


- Personería Auxiliar (Gestión de Informática) deberá garantizar que la información a ser entregada a los terceros proveedores o desarrolladores de sistemas de información para sus pruebas será enmascarada y no corresponderá a datos de los ambientes de producción.
- Personería Auxiliar (Gestión de Informática) deberá eliminar la información de los ambientes de pruebas una vez están concluidas.
- Personería Auxiliar (Gestión de Informática) deberá generar una metodología de pruebas al software desarrollado que contenga pautas para la selección de escenarios, niveles, tipo, datos de prueba sugerencias de documentación.

#### **9.11. Seguridad de la información en las relaciones con los proveedores o terceros**

La Personería de Medellín establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los mismos, cumplan con las políticas, normas y procedimientos de seguridad de la información. Los funcionarios o contratistas responsables de la realización o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

##### **9.11.1. Política de seguridad de la información para las relaciones con los proveedores**


- Para los servicios contratados con proveedores en los cuales se requiera del intercambio de información institucional, se deben establecer Acuerdos de Confidencialidad y de intercambio de información en los que se definan claramente los requerimientos de seguridad de la información, incluida la obligación de cumplir con lo establecido en el presente manual y sus respectivas cláusulas civiles y penales en caso de incumplimientos.
- El responsable del activo de información deberá definir la finalidad de la autorización de acceso a la información que se otorgue al proveedor y documentar la autorización del acceso a los datos de acuerdo con el fin previsto.
- Siempre que se otorgue acceso a la información de la Personería de Medellín a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de la Entidad y las cláusulas requeridas para proteger la información a acceder.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 58  | de       | 65      |     |      |

- Los proveedores de la Personería de Medellín deberán cumplir las políticas de seguridad en cuanto a la confidencialidad de la información de la Entidad.
- Personería Auxiliar (Gestión de Informática) establecerá con los proveedores Acuerdos de Niveles de Servicio (ANS) con sus respectivas penalizaciones en caso de incumplimiento de los niveles acordados para cada servicio contratado, y realizará el seguimiento periódico de los mismos.
- Personería Auxiliar (Gestión de Informática) y la oficina de Gestión Jurídica deberán generar un modelo base para los Acuerdos de Niveles de Servicio (ANS) y requisitos de seguridad de la Información, con los que deben cumplir los proveedores de servicios; este modelo debe ser divulgado a todas las áreas que adquieran o supervisen recursos o servicios tecnológicos.
- Antes de conceder acceso a la información institucional de la Entidad se deberá dar a conocer el presente manual a los proveedores a los cuales se otorgará el permiso.
- Antes de conceder permisos de acceso a la información a los proveedores, el responsable del activo deberá analizar la justificación de la necesidad del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso y los controles mínimos de seguridad a tener en cuenta frente al tratamiento de la información.
- Solo se dará acceso a los sistemas de información o áreas seguras de la Entidad hasta que se haya formalizado la relación contractual y firmado el Acuerdo de Confidencialidad con los proveedores.
- En contratos y acuerdos que se establezca con proveedores, se deberá considerar y dar tratamiento a los riesgos de seguridad de la información asociados con el cumplimiento de las obligaciones contractuales, la calidad de los productos y servicios adquiridos y la seguridad de la información institucional.
- Personería Auxiliar (Gestión de Informática) deberá mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica.

#### 9.11.2. Gestión de la prestación de servicios de proveedores

- La Personería de Medellín será responsable de hacer el seguimiento periódico, supervisar por el cumplimiento de las obligaciones contractuales y la calidad de los productos y servicios, así como el cumplimiento de los Acuerdos de Niveles de Servicio establecidos con sus proveedores.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 59  | de       | 65      |     |      |


- Personería Auxiliar (Gestión de Informática) será la encargada de aprobar los cambios que deban realizar sus proveedores durante la prestación de los servicios, garantizando los principios de seguridad de la información y teniendo en cuenta la criticidad del servicio afectado.
- Los proveedores de productos o servicios de la Personería de Medellín deben abstenerse de realizar cambios que afecten la prestación de los servicios contratados con la Entidad o generen riesgo para la seguridad de la información institucional, sin previo aviso y autorización del Personería Auxiliar (Gestión de Informática) .
- Personería Auxiliar (Gestión de Informática) deberá verificar el momento pertinente para que el proveedor realice la conexión, apegándose a las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la institución.
- Los terceros que se conecten la red de datos corporativa de la Entidad están obligados a seguir las políticas, normas y procedimientos de seguridad existentes.
- Los terceros que tengan o traigan equipos de cómputo a la Entidad deben reportar al Personería Auxiliar (Gestión de Informática) indicando los componentes de hardware que posea; además de una copia de las licencias del software instalado en cada equipo. Por ningún motivo se aceptará en la Entidad software no licenciado.
- La Personería de Medellín no asumirá ninguna responsabilidad por pérdida de equipos de cómputo propiedad de terceros, ni por la información almacenada en dichos equipos.

## 9.12. Gestión de Incidentes de Seguridad de la Información

La Personería de Medellín promoverá entre los funcionarios, contratistas y terceros el reporte de incidentes relacionados con la seguridad de la información y de procesamiento, incluyendo cualquier tipo de almacenamiento de información, como la plataforma tecnológica, los sistemas de información y procesamiento, los medios físicos de almacenamiento y las personas.

### 9.12.1. Gestión de incidentes y mejoras en la seguridad de la información

- El designado por Personería Auxiliar asignará responsabilidades y procedimientos para el tratamiento de los incidentes de seguridad de la información, de acuerdo con las competencias, responsabilidades y los activos a su cargo; para asegurar una respuesta rápida, organizada y efectiva.
- Los propietarios de los activos de información deberán informar al designado por Personería

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 60  | de       | 65      |     |      |

Auxiliar los incidentes de seguridad que hayan identificado.

- El designado por Personería Auxiliar deberá evaluar los incidentes de seguridad de acuerdo con sus situaciones particulares y escalar aquellos en los que se considere pertinente.

El designado por Personería Auxiliar deberá designar personal calificado para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una exploración exhaustiva, proporcionando las soluciones y finalmente previendo su recurrencia.


- El designado por Personería Auxiliar deberá crear una base de conocimientos y lecciones aprendidas para los incidentes de seguridad presentados con sus respectivas soluciones con el fin de reducir el tiempo de respuesta para los incidentes futuros.
- Personería Auxiliar (Gestión Contractual, Gestión del Talento Humano, Gestión Informática y Bienes Logísticos) de los activos afectado durante un incidente de seguridad, serán los encargados del seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como de su comunicación al jefe inmediato y a los propietarios de la información afectada.
- Todo evento que se clasifique como un incidente de seguridad, debe ser documentado y tratado de forma inmediata y de acuerdo con los procedimientos formalmente implementados por la Entidad.
- Todos los funcionarios y contratistas de la Entidad deberán reportar de manera oportuna a el Personería Auxiliar (Gestión de Informática), las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.

### 9.13. Seguridad de la Información en la Gestión de la Continuidad del Negocio

La Personería de Medellín proporcionará los recursos para proveer una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la Entidad y que afecten la continuidad de su operación; así mismo, velará por la seguridad de la información durante la ocurrencia de eventos catastróficos.


#### 9.13.1. Continuidad de seguridad de la información

- Personería Auxiliar (Gestión de Informática) deberá realizar los análisis de impacto al negocio de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- La responsabilidad de poner en marcha del plan de contingencias será del líder de cada proceso y

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 61  | de       | 65      |     |      |

deberá entrenar a todo el personal involucrado en su utilización.

- El designado por Personería Auxiliar deberá seleccionar las estrategias de recuperación más convenientes para la Entidad.
- Los planes deberán incluir procedimientos de emergencia, escenarios de contingencia, responsabilidades asignadas, directorio de contactos, plan de capacitación, plan de comunicaciones, plan de adquisiciones, plan de pruebas, entre otros
- Personería Auxiliar (Gestión de Informática) deberá identificar y designar responsables que deben actuar en momentos de emergencia o desastre, dichos responsables deberán ser capacitados en las actividades a realizar y los procedimientos a seguir en caso de un evento catastrófico.
- Personería Auxiliar (Gestión de Informática) formulará los planes, controles y procedimientos necesarios, para asegurar la continuidad de las operaciones en las cuales se de tratamiento a la información institucional de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) deberá garantizar la realización de pruebas periódicas del plan de recuperación ante desastres, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
- Personería Auxiliar (Gestión de Informática) deberá proveer un plan de recuperación ante desastres para los centros de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios prestados y sistemas previstos.
- Los planes deberán incluir procedimientos de emergencia, escenarios de contingencia, responsabilidades asignadas, directorio de contactos, plan de capacitación, plan de comunicaciones, plan de adquisiciones, plan de pruebas, entre otros.
- Los sistemas de información existentes y los nuevos que se pongan en funcionamiento deberán incluir como un requisito para su puesta en funcionamiento, el desarrollo del respectivo plan de contingencias para garantizar su continuidad.
- Para garantizar la continuidad en el funcionamiento de las aplicaciones se debe garantizar al menos una persona adicional al Líder del proceso que pueda cumplir este rol, y así evitar traumatismos en caso de ausencia temporal o definitiva del titular de este cargo.


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 62  | de       | 65      |     |      |

#### 9.14. Cumplimiento

La Personería de Medellín velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas la referente a derechos de autor y propiedad intelectual, razón por la cual estará pendiente de que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

##### 9.14.1. Cumplimiento de requisitos legales y contractuales

- La oficina de Gestión Jurídica y el Personería Auxiliar (Gestión de Informática) identificará, documentará, actualizará cuando sea necesario, y dará cumplimiento a la normatividad y requisitos legales relacionados con la seguridad de la información, que estén directamente relacionados con el ejercicio de sus funcionarios y contratistas.
- Se deberá implementar mecanismos o procedimientos para evitar el incumplimiento de las normas de propiedad intelectual, derechos de autor y el uso de software patentado.
- Personería Auxiliar (Gestión de Informática) estará autorizada para buscar programas instalados en los equipos de la Entidad sin autorización y procederá con la desinstalación inmediata de los mismos.
- Las licencias de uso de software estarán bajo custodia del Personería Auxiliar (Gestión de Informática) . Al igual los manuales y los medios de almacenamiento (CD, cintas magnéticas, dispositivos, entre otros), que acompañen a las versiones originales de software.
- Personería Auxiliar (Gestión de Informática) es la única área autorizada para realizar copia de seguridad del software original, cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización puede conllevar a las sanciones administrativas y legales pertinentes.
- El software adquirido por la Personería de Medellín no puede ser copiado o suministrado a terceros sin la debida autorización de la Personería Auxiliar (Gestión de Informática) y sin que se suscriba algún tipo de contrato o convenio por parte de la Personería de Medellín y el tercero.
- Se prohíbe el uso e instalación de juegos, software pirata o que aun siendo software libre no esté autorizado por el Personería Auxiliar (Gestión de Informática) para su uso.
- Se prohíbe el acceso y consulta de páginas web o material pornográfico en los computadores de la Entidad. Así mismo está prohibido almacenar archivos de música o videos o cualquier otro elemento que requiera para su uso de una licencia relacionada con derechos de propiedad

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 63  | de       | 65      |     |      |

intelectual, patentes o similares.


- Los funcionarios, contratistas o terceros responsables de la publicación de la información en los sitios web e Intranet de la Entidad, deberán atender el cumplimiento a las normas en materia de propiedad intelectual y demás políticas establecidas en el presente manual, y en ninguna circunstancia deben publicar información sensible, reservada o confidencial que se encuentre en poder de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) podrá autorizar el uso de material o software declarado como de uso libre, el producido por ella misma o el producido por el titular o propietario externo cuando participe autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente; para esto el Personería Auxiliar (Gestión de Informática) se asegurará que el software cumpla con los requisitos mínimos de seguridad y licenciamiento para su uso.

#### 9.14.2. Revisiones de seguridad de la información

- Personería Auxiliar (Gestión de Informática) verificará permanentemente el cumplimiento de los controles, procedimientos y directrices establecidos en el Sistema de Gestión de Seguridad de la Información – SGSI de la Personería de Medellín.
- Personería Auxiliar (Gestión de Informática) deberá gestionar la verificación del cumplimiento del Manual del Sistema de Gestión de Seguridad de la Información.
- Personería Auxiliar (Gestión de Informática) podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo. El mal uso de los recursos informáticos que sea detectado será reportado.
- Los jefes de área como dueños de los procesos establecidos en la Entidad deberán apoyar las revisiones del cumplimiento de las políticas de seguridad de la información que les competa y cualquier otro requerimiento de seguridad.
- Personería Auxiliar (Gestión de Informática) tendrá como una de sus funciones proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de las bases de datos de información automatizada en general.

#### 9.14.3. Privacidad y protección de información de datos personales

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de


|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 64  | de       | 65      |     |      |

datos personales, la Personería de Medellín velará por la protección de los datos personales de los funcionarios, contratistas, proveedores, usuarios y demás terceros de los cuales reciba y administre información, como consta en la Resolución 043 de 30 de enero de 2018 “Por medio de la cual se adopta la Política de Privacidad y procedimientos para la protección de datos”.

- Se establecerán los términos, condiciones y finalidades para las cuales la Entidad como responsable de los datos personales obtenidos en sus distintos canales, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla, hayan suministrado datos personales.
- Así mismo buscará proteger la privacidad de la información personal de sus funcionarios y contratistas, estableciendo los controles necesarios para preservar aquella información que la Entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la Entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.
- Las áreas que procesan datos personales de funcionarios, contratistas, usuarios y terceros deberán obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la institución.
- Las áreas que procesan datos personales de funcionarios, contratistas, usuarios y terceros deberán asegurar que solo aquellas personas que tengan una relación laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de funcionarios, contratistas, usuarios y terceros deberán acoger las directrices técnicas y procedimientos establecidos para enviar mensajes por correo electrónico a dichos usuarios.
- Personería Auxiliar (Gestión de Informática) debe establecer los controles para el tratamiento y protección de los datos personales de los funcionarios, contratistas, usuarios y terceros de los cuales reciba y administre información almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación, sin la autorización requerida.

#### **ACTUALIZACION DE LAS POLITICAS DE USO Y MANEJO DE INFORMACIÓN**

Es responsabilidad de LA PERSONERIA AUXILIAR en coordinación con el designado por Personería Auxiliar (Gestión de Informática) liderar la actualización de las presentes políticas de acuerdo con las necesidades de la Entidad y al avance tecnológico del medio, dicha actualización será por versiones para garantizarla vigencia de estas en el tiempo.

|   |   |          |         |     |      |
|---|---|----------|---------|-----|------|
|  | <b>SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION</b>        | CODIGO   | MSSI001 |     |      |
|   |   | VERSION  | 1       |     |      |
|   | <b>MANUAL POLITICAS DE SEGURIDAD DEL SISTEMA DE INFORMACION</b> | VIGENCIA | DIA     | MES | AÑO  |
|   |   |          | 8       | 9   | 2021 |
| Página  | 65  | de       | 65      |     |      |

| 2. RESPONSABLES DE LAS COPIAS CONTROLADAS |          |          |                         |
|---|----------|----------|-------------------------|
| Nº COPIA                                  | EMPLEO   | COPIA EN |                         |
|   |          | PAPEL    | ELECTRÓNICA EN INTRANET |
| 1   | Intranet |          | X                       |

| 3. HISTORIAL |            |       |     |      |  |
|--------------|------------|-------|-----|------|--|
| VERSIÓN      | RESOLUCIÓN | FECHA |     |      | NATURALEZA CAMBIO  |
|              |            | DÍA   | MES | AÑO  |  |
| 1            | 320        | 8     | 9   | 2021 | Implementación del Sistema de Seguridad y Privacidad de la Información |

PROPIEDAD INTELECTUAL  
PERSONERÍA DE MEDÉLLIN