MANUAL DE POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. GENERALIDADES

1.1. AMBITO DE APLICACIÓN

Las políticas de Seguridad de la Información son de obligatorio para todos los servidores públicos del Área Metropolitana de Barranquilla. La falta de observancia a cualquiera de ellas, tendrá como consecuencia la aplicación de las medidas consideradas necesarias por la Secretaría General de la Entidad.

1.2. INTRODUCCIÓN

La Información en las Entidades existen de diversas formas: impresa, escrita en papel, electrónicamente o digital, proyectada, en grabaciones o en forma oral.

La Seguridad de la Información consiste en la protección de la Información contra las múltiples amenazas que puedan dañarla o afectarla con el fin de garantizar la continuidad de la operación, minimizar los riesgos institucionales y maximizar las oportunidades de la organización.

1.3. OBJETIVOS

1.3.1. Objetivo General

Establecer lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información del **ÁREA METROPOLITANA DE BARRANQUILLA**, teniendo en cuenta los procesos, la operación los objetivos y los requisitos legales vigentes en la Entidad.

1.3.2. Objetivos Específicos

- Definir la Política de Seguridad de la Información del ÁREA METROPOLITANA DE BARRANQUILLA.
- Dar cumplimiento y conformidad a la normatividad, leyes y regulaciones que le aplican al ÁREA METROPOLITANA DE BARRANQUILLA en el desarrollo de su misión.

- Plasmar las directrices en materia de Seguridad de la Información con el fin de proteger los activos de la Información del **ÁREA METROPOLITANA DE BARRANQUILLA.**

- Fortalecer la cultura de Seguridad de la Información en funcionarios, contratistas y terceros del ÁREA METROPOLITANA DE BARRANQUILLA, a través de la definición de una estrategia de uso y apropiación de la Política.

1.4. ALCANCE

Este manual de Seguridad de la Información es una Política que apoya al Plan de Seguridad y Privacidad de la Información estructurado por los lineamientos impartidos por el Modelo Integral de Planeación y Gestión.

Esta Política es de consideración por parte de los funcionarios y contratistas del ÁREA METROPOLITANA DE BARRANQUILLA.

1.5. RESPONSABILIDADES

- El Equipo Directivo es el responsable de asegurar que la Seguridad de la Información se gestiona adecuadamente en toda la organización.
- Cada jefe de área es responsable de garantizar que las personas que trabajan en su equipo de trabajo protegen la información de acuerdo con las normas establecidas.
- El responsable de la Seguridad de la Información asesora al equipo directivo proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- Cada Servidor Público tiene la responsabilidad de mantener la Seguridad de la Información dentro de las actividades relacionadas con sus actividades.

1.6. MARCO REGULATORIO Y NORMATIVO

El Área Metropolitana de Barranquilla, como entidad pública, se encuentra regulada por un marco normativo y regulatorio relacionado con la Seguridad de la Información, especialmente dada por el Modelo Integrado de Planeación y Gestión – MIPG, especialmente la Estrategia de Gobierno Digital, que se evidencia en el Decreto Único Reglamentario del Sector de la Tecnologías de la Información y las Comunicaciones 1078 de 2015, el cual comprende entre sus propósitos, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.

A continuación, se relacionan las demás normas, leyes, decretos y resoluciones que aplican para el establecimiento, implementación y operación de la Política de Seguridad de la Información en el ÁREA METROPOLITANA DE BARRANQUILLA:

- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Decreto 2693 de 2012**: Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
- **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **NTC-ISO/IEC 27001 – 27002: 2013:** Norma Técnica Colombiana TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.

Norma Técnica Colombiana TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).

- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 415 de 2016:** Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- **Decreto 1414 de 2017:** Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones.
- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

EL **ÁREA METROPOLITANA DE BARRANQUILLA** establece las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la entidad en cuanto a la protección de sus activos de Información.

1.6.1. CONSIDERACIONES GENERALES

a) La protección de la información y de los recursos relacionados con la misma, son considerados parte vital del desarrollo de las distintas funciones y actividades que diariamente se ejecutan en la entidad.
b) El contenido del presente documento, es un manual para la protección de la información de la entidad basada en una Política de Seguridad que se extiende a cualquier información sensible, ya sea la contenida en correos electrónicos, escritos de distintas denominaciones (jurídicos, técnicos, financieros, reportes, información sobre los usuarios y empleados, archivos de computador, conservaciones y microfichas).
c) La mejor protección de la información es ser consciente de la necesidad de su seguridad y de las responsabilidades individuales que se contraen, contra su alteración, destrucción y revelación. Por consiguiente, cuando la información de uso diario no se encuentra disponible o no es confiable, las actividades diarias de la entidad se verán afectadas negativamente.
d) El Asesor 105-01 de la Oficina de Información y Comunicación, del área de Sistemas es quien vela directamente por la Seguridad de la Información de la Entidad y estable e implementar mecanismos para realizar las copias de seguridad de la información institucional, monitorear las cámaras de seguridad, configurar y administrar el Software de Protección Antivirus, configurar y administrar los usuarios del Servidor de dominio, administrar el acceso a los contenidos de Internet, otorgar y quitar permisos especiales sobre dichos contenidos.

El Área Metropolitana de Barranquilla asume el compromiso de implementar hasta donde su disponibilidad lo permita, medidas y estrategias para proteger los activos de información de la Entidad, estableciendo lo siguiente:

1.6.2. DE APLICACIÓN GENERAL

a) El acceso físico a la Infraestructura Tecnológica, como Servidor de Dominio y Aplicaciones, DVR, Planta Telefónica, UPS, etc., será protegida mediante

cuarto aislado y puerta con cerradura independiente, las cuales serán custodiadas por el personal de la Oficina de Información y Comunicación, del área de Tecnología o Sistemas. Con el fin de proteger la Información Institucional y la configuración de la misma que reposa en dicha infraestructura.

b) El personal de la Oficina de Información y Comunicación, del área de Tecnología, estará ubicado físicamente un tanto aislado del resto del personal y en lo posible en un área que cuente con puerta con cerradura para minimizar y/o controlar el acceso de personal ajeno al área, que pueda por error, intención o sin intención alterar la información contenida en las Bases de Datos de los distintos Sistemas de Información de la Entidad.

c) El acceso lógico a las Bases de Datos y Sistemas de Información, están protegidos por credenciales de acceso como Usuario y Contraseña. Los usuarios autorizados para acceder a las Bases de Datos, con el personal de la Oficina de Información y Comunicación del área de Tecnología, funcionarios y contratistas cuyo objeto de contrato esté directamente relacionado con el apoyo a la gestión de la Oficina y orientado al manejo de Información de los Sistemas de Información de la Entidad.

d) Las responsabilidades frente a la Seguridad de la Información deben ser aceptadas por cada uno de los empleados, proveedores y terceros que intervengan con la Entidad.

e) Todos los usuarios de los recursos informáticos institucionales de la entidad deberán sujetarse a las Políticas de Seguridad de la Información establecidas en el presente documento y demás documentación relacionado con la misma.

f) Los Servidores públicos de la Entidad deben usar la Información del ÁREA METROPOLITANA DE BARRANQUILLA únicamente para propósitos del negocio autorizado y en cumplimiento de su labor.

g) Todos los Servidores Públicos deben respetar la confidencialidad de la Información del ÁREA METROPOLITANA DE BARRANQUILLA.

h) Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

i) Es responsabilidad de todos los funcionarios y contratistas del **ÁREA METROPOLITANA DE BARRANQUILLA** reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de la información que identifique.

j) La Entidad debe tener en cuenta las Categorías de la Clasificación de la Información, entre las cuales se encuentran las siguientes: **GENERAL. –** Esta información debe ser emitida por la entidad, divulgada, publicada y fácilmente observada desde cualquier lugar. **INTERNA**. – Es creada y usada por los empleados de la entidad incluyendo la confiada por un socio institucional. Los empleados de la entidad accesarán a esta información con la prohibición de no publicarla o revelarla sin excepción alguna. La destrucción de esta información por motivos de seguridad, debe ser realizada bajo las mejores garantías posibles. **CONFIDENCIAL**. – Se accede a esta información a través de un mecanismo de control de autorizaciones, otorgado por quien tiene las facultades para ello. El uso inapropiado de esta información puede causar daños financieros, violación a la legalidad y a la imagen de la entidad, a los usuarios, proveedores y empleados en general.

k) Mientras demora el atascamiento de hojas en la fotocopiadora o impresora, es obligatoria la permanencia del responsable de su manejo hasta el destrabamiento para garantía de la vigilancia de la información. Es necesario verificar en la fotocopiadora o impresora que no queden copias adicionales a su interior.

l) Es obligatorio asegurar los documentos originales que se entregan para fotocopiar.

1.6.3. DE APLICACIÓN POR PARTE DE LA OFICINA DE INFORMACIÓN Y COMUNICACIÓN

a) Verificar que la información institucional producida y recibida en la entidad se encuentre siempre disponible y salvaguardada. Siempre y cuando ésta se encuentre ubicada en la ruta que se ha definido para su almacenamiento Institucional y disposición de copia de seguridad – Ruta: Mis Documentos de cada computador).

b) Custodiar la Infraestructura Tecnológica de la Entidad, haciendo uso adecuado de la llave otorgada y manipulación de los elementos que contienen la Información de la Entidad.

c) Hacer uso adecuado de los permisos y accesos a las Bases de Datos y Sistemas de Información del AMB, protegiendo siempre la integridad de la misma.

2. POLITICAS Y NORMAS ESPECÍFICAS SOBRE USO DE ACTIVOS DE INFORMACIÓN

2.1.1. DE APLICACIÓN GENERAL

a) El Servidor Público es responsable del uso de los recursos de la información, en tanto, es su obligación cumplir con las Políticas de Seguridad de la Información de la entidad, Estándares y Procedimientos, así mismo, de participar activamente en los programas de concientización de la seguridad de la información.
b) Está prohibido deshabilitar o evadir los controles de seguridad del sistema de computación, acceder a una cuenta de correo electrónico asignada a otro funcionario, a excepción del caso que un ente de control solicite los correos electrónicos para el desarrollo de alguna investigación en curso acerca de un servidor público o ex servidor público de la Entidad, usar los activos de información de la entidad para acceder ilegalmente a cualquier sistema interno o externo y realizar reenvíos de mensajes de correo electrónico a cualquier dirección externa o interna.
c) Entre los múltiples procederes a los que se debe recurrir para proteger la información, se recomienda: - El almacenamiento de toda la información en sitios o archivadores herméticos con ofrecimiento de alta garantía de seguridad y en espacios controlados para el acceso. – Prohibir la discusión del contenido de información en lugares externos a las oficinas de la entidad, ante la susceptibilidad de violar la confidencialidad aún entre familiares. – Prevenir a quienes conociendo la información almacenada la difundan por imprevisión o descuido.
d) La información contenida en los equipos de cómputo de la entidad, debe ser protegida con dispositivos y mecanismos de seguridad, tales como contraseñas.
e) No compartir perfiles de usuario, contraseñas sesiones en estaciones de trabajo, documentos, o cualquier tipo de información confidencial. En caso de compartir las contraseñas a Sistemas de Información o Equipos de Cómputo, la responsabilidad recaerá sobre el propietario de dicho usuario.
f) No anotar y/o almacenar en lugares visibles las contraseñas de acceso a los Sistemas de Información.
g) Las contraseñas diseñas por cada funcionario para el acceso a los equipos de cómputo deben ser difíciles de descubrir o acertar y deben ajustarse a

los parámetros mínimos que tiene configurado el Servidor de Dominio de la entidad.

h) La información de la entidad tanto producida como recibida que se encuentre en los equipos de cómputo de cada funcionario, debe ser guardada en la Carpeta llamada ***Mis Documentos***, que se encuentra en cado uno de los computadores. Con el fin de poder ubicar fácilmente la información relacionada con la entidad al momento de realizar las copias (Back up) de información, y evitar de esta manera guardar información personal de los funcionarios o que no esté relacionada con la institución.

2.1.2. DE APLICACIÓN DE LA OFICINA DE INFORMACIÓN Y COMUNICACIÓN

a) Es obligatoriedad realizar copias o back up de la información de la entidad, contenida en los diferentes equipos de cómputo de los funcionarios, so pena de la obligatoria reconstrucción de la información pérdida.
b) Es obligatoriedad configurar el Servidor de Dominio, de tal manera que exija el cambio de contraseña de los equipos de cómputo, cada (30) días, con los siguientes parámetros: La contraseña debe estar compuesta al menos de ocho (8) caracteres, debe contener caracteres alfanuméricos, numéricos y al menos un (1) carácter especial.
c) Es obligatoriedad implementar un procedimiento para realizar copia de seguridad de la información institucional, con base en la política establecida.

3. POLITICAS Y NORMAS ESPECÍFICAS SOBRE MEDIDAS DE SEGURIDAD FISICA, LOGICA Y CONFIDENCIALIDAD DE LA INFORMACIÓN

3.1.1. DE APLICACIÓN GENERAL

a) Cada usuario se responsabilizará de salvaguardar la integridad de la información a su cargo, mediante la utilización de contraseñas y cumplimiento de las Políticas de Seguridad de la Información.
b) La sesión de los equipos de cómputo de la entidad debe ser bloqueada por el funcionario a cargo del equipo, al momento de ausentarse de su puesto de trabajo, con el fin de evitar el acceso a la información sensible de la entidad, por un tercero.

c) Todos los usuarios de la información institucional y el personal de la Oficina de Información y Comunicación deberán sujetarse a las Políticas para la Seguridad de la Información establecidas por la Entidad.
d) En cuanto a la Seguridad Física de la Información los usuarios deben adoptar la buena práctica de guardar los documentos físicos en los elementos dispuestos para tal fin como archivadores, carpetas, sobres, etc., evitando dejar documentos en sus escritorios de trabajo, ya que, de esta forma se aumenta la probabilidad de pérdida o extracción de información que puede ser sensible.
e) Las instalaciones de la Entidad, contarán con cámaras de vigilancia que cubran el mayor número de área para poder monitorear de esta forma los movimientos realizados a nivel interno de la Entidad y poder revisar lo sucedido en caso que se llegue a presentar pérdida de información.
f) El monitoreo de las Cámaras de Seguridad está a cargo del Jefe Administrativo de la Oficina Administrativa y el Asesor de la Oficina de Información y Comunicación, del área de Sistemas.

3.1.2. DE APLICACIÓN DE LA OFICINA DE INFORMACIÓN Y COMUNICACIÓN

a) Es obligatoriedad la protección de la información contenida en los equipos de cómputo de la entidad, mediante la adquisición e instalación de un Sistema de Protección (Software) de Antivirus Corporativo administrable.
b) Se inactivará el acceso a los Sistemas de Información de los usuarios en el periodo que se encuentren de vacaciones o incapacidad, según previa notificación de las novedades de los usuarios, por parte del área de Talento Humano, a través de e-mail institucional. En caso que el área competente, no reporte a la Oficina de Información y Comunicación esos periodos de ausentismo, NO es responsabilidad de dicha oficina la inactivación de dichos usuarios.
c) Ser responsable de conocer, solicitar, ratificar los privilegios de acceso a los empleados que le sean reportado por cada jefe de área.
d) Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad, tales como el centro de datos del AMB.
e) Conservar los registros de los empleados con privilegios de acceso a la información.

g) No se hará responsable por la información que se pierda en el proceso de erradicación de virus y/o software pirata.

4. POLITICAS Y NORMAS ESPECÍFICAS SOBRE EL USO DEL SERVICIO DE ACCESO A INTERNET

a) El Área Metropolitana de Barranquilla provee el servicio de Internet como herramienta de trabajo para sus usuarios.

b) El acceso al contenido de Internet está restringido para acceder a redes sociales o sitios que proporcionen información que genere distracción al usuario y no aporten contenido a la ejecución de los procesos corporativos que el servidor público requiera.
Sin embargo, en la eventualidad que un jefe de área requiera que un servidor público de su equipo de trabajo, requiera acceso especial a dichos sitios, deberá solicitar por escrito al Jefe Administrativo del AMB su autorización y este a su vez, indicar a la Oficina de Información y Comunicación que otorgue dichos permisos al funcionario indicado.

c) El Asesor de la Oficina de Información y Comunicación, del área de Sistemas, es quien podrá cambiar los permisos de navegación previa autorización del Jefe Administrativo.

5. POLITICAS Y NORMAS ESPECÍFICAS SOBRE DIVULGACIÓN DE LA INFORMACIÓN

5.1.1. DE APLICACIÓN GENERAL

a) En los viajes oficiales o personales, el funcionario o ex funcionario debe tomar precauciones aún más drásticas que las adoptadas en la entidad para la seguridad de la información. Deben portarse únicamente los documentos y materiales estrictamente necesarios.

b) Ante la eventualidad de extravío, se recomienda guardar celosamente un duplicado original de la información considerada valiosa por la entidad.

c) Es obligatorio para cualquier funcionario reportar ante un superior jerárquico cualquiera de los hechos siguientes: 1. Cuando alguien se niegue a exhibir la debida autorización y no obstante pretenda información relacionada de la entidad, 2. Cuando se observa que una información sensible se encuentra desprotegida, 3. Cuando se observa que la falta de una información

sensible o colocada riesgosamente, 4. Cuando los escritorios, equipos de cómputo, archivos o cualquier otro bien público, ha sido objeto de violencia, 5. Cuando existan personas extrañas indagando temas sensibles de la entidad, o en actitud sospechosa tomando fotografías no autorizadas, 6. Cuando se hagan reproducciones no autorizadas de información sensible, 7. Cuando sucedan incidentes causados por virus informáticos.

d) Bajo ninguna circunstancia se puede revelar los conocimientos de hechos y contenidos de información y confidencialidad adquiridos por el funcionario durante su vinculación con la entidad, tal responsabilidad legal, continúa hasta cinco (5) años después del retiro del funcionario de la entidad, sin consideración a las razones que caracterizaron al mismo.

6. POLITICAS Y NORMAS ESPECÍFICAS SOBRE EL MANEJO DE DOCUMENTOS ELECTRÓNICOS

6.1.1. DE APLICACIÓN GENERAL

a) Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del ÁREA METROPOLITANA DE BARRANQUILLA. Los mensajes de correo electrónico corporativo deben ser manejados como una comunicación privada y directa entre emisor y receptor, conservando la decencia y respecto del comunicado.
b) Las comunicaciones electrónicas en lo posible deben ser concretas, precisas y completas.
c) La información solicitada mediante correo electrónico corporativo debe ser tratada como información de la Entidad y proteger siempre su integridad.
d) Las comunicaciones electrónicas oficiales hacían el exterior de la deberán ser firmadas por el nombre completo del funcionario, cargo y oficina. En lo posible, ser enviado por el jefe del área.

7. CONTROL DE CAMBIOS			
FECHA	**VERSION**	**DESCRIPCION DEL CAMBIO**	**APROBADO POR**
24/08/2015	1	Creación documento	Jefe Administrativa
29/10/2020	2	Actualización del documento	Jefe Administrativa/Comité Institucional de Gestión y Desempeño