# 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 sanciones disciplinarias correspondientes.

## 1.2. POLITICAS GENERALES

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.

### 1.2.1. CONSIDERACIONES GENERALES

a) La protección de la información y de los recursos relacionados con la misma, son considerados como parte vital del desarrollo de las distintas funciones y actividades que diariamente se ejecutan en la entidad.
b) El contenido de la presente resolución 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, faxes, 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.

### 1.2.2. DE APLICACIÓN GENERAL

a) Todos los usuarios de los recursos informáticos institucionales y el personal de la Oficina de Organización, Métodos y Procedimientos deberán sujetarse a las políticas de seguridad establecidas.

b) La Oficina de Organización, Métodos y Procedimientos y la Oficina de Control Interno de la entidad vigilarán que se acaten las Políticas de Seguridad de la Información vigentes.
c) Los usuarios participarán activamente de todas y cada una de las etapas del proceso de sistematización del área al que pertenece y/o del proceso correspondiente.
d) 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.
e) Es obligatorio asegurar los documentos originales que se entregan para fotocopiar.
f) Los faxes recibidos que contengan información relevante deben ser recogidos prontamente y evitar así la posibilidad de que su contenido sea revelado.
g) Está prohibido enviar por fax información confidencial de la entidad.

### 1.2.3. DE APLICACIÓN POR PARTE DE LA OFICINA DE ORGANIZACIÓN, MÉTODOS Y PROCEDIMIENTOS

a) Verificará que la información institucional producida y recibida en la entidad se encuentre siempre disponible y salvaguardada.
b) Mantendrá el derecho de los usuarios a la confidencialidad de correo electrónico.
c) En los casos que se detecten acciones que puedan poner en riesgo la seguridad o los niveles de eficiencia, tanto de la red de datos institucional como de cualquiera de los componentes de la misma, la Oficina de Organización, Métodos y Procedimientos podrá realizar una auditoría en coordinación con la Oficina de Control Interno y emitir recomendaciones para prevenir o corregir estas situaciones.
d) El ÁREA METROPOLITANA DE BARRANQUILLA definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

e) 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.
f) 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.
g) 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.

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

### 2.1.1. DE APLICACIÓN GENERAL

a) El funcionario 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, Estandares 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, accesar a una cuenta de correo electrónico asignada a otro funcionario, usar los activos de información de la entidad para accesar 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 ola 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. (Guayas, contraseñas, etc.).

e) Se prohíbe accesar a información confidencial de la entidad, en lugares públicos.

f) 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.

g) Se prohíbe compartir las contraseñas de los sistemas de información y de los equipos de cómputo, así como anotarlas en lugares visibles o de fácil acceso.

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.

i) Con el fin de poder realizar las copias de seguridad de la información de la entidad contenida en los diferentes equipos de cómputo, sin afectar el rendimiento de la red, todos los usuarios, deberán apagar diariamente, los equipos de cómputo al momento de marcharse de la entidad. Dicha acción activará automáticamente la copia de seguridad del equipo, una vez se implemente el procedimiento de Back Up en la entidad.

j) Cabe resaltar que, equipo que no sea apagado por su responsable, no se le podrá realizar back up de la información, y es total y absoluta responsabilidad del funcionario a cargo, de responder por la información contenida en éste.

### 2.1.2. DE APLICACIÓN DE LA OFICINA DE ORGANIZACIÓN, MÉTODOS Y PROCEDIMEINTOS

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 Organización, Métodos y Procedimientos deberán sujetarse a las políticas para la seguridad de la información establecidas por la entidad.

### 3.1.2. DE APLICACIÓN DE LA OFICINA DE ORGANIZACIÓN, MÉTODOS Y PROCEDIMIENTOS

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.

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 de la Oficina de Talento Humano, a través de e-mail institucional.

d) La Información debe ser clasificada según su nivel de sensibilidad a la confidencialidad, disponibilidad e integridad (pérdida o daño), volumen y criticidad, con el fin de priorizar el back up y la recuperación de la misma.

e) 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 servicio de Internet está restringido por las políticas de seguridad establecidas por la Oficina de Organización, Métodos y Procedimientos de la entidad.

c) Está prohibido conectarse a redes o sitios web no autorizados. En caso de requerir el acceso a sitios web o redes por fines institucionales, debe solicitar autorización previa del jefe administrativo, quien evaluará la justificación y responderá a la solitud del funcionario; en caso, de aceptarlo, deberá dar instrucciones al asesor de sistemas encargado de la administración del acceso a Internet para que proceda a otorgar el permiso.

d) Se tomarán acciones disciplinarias contra usuarios que infrinjan las políticas establecidas en este documento con respecto al uso del Servicio de acceso a Internet.

## 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.

| X. CONTROL DE CAMBIOS | | | |
|---|---|---|---|
| **FECHA** | **VERSION** | **DESCRIPCION DEL CAMBIO** | **APROBADO POR** |
| 24/08/2015 | 1 | Creación documento | Jefe Administrativa |
| | | | |