ÁREA METROPOLITANA DE BUCARAMANGA

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - ÁREA METROPOLITANA DE BUCARAMANGA

Apoyo tecnológico de la información - Gestión corporativa
Año 2021

# Tabla de Contenido

# 1. INTRODUCCIÓN

El Área Metropolitana de Bucaramanga es una entidad administrativa formada por un conjunto de cuatro Municipios, dotada de personería jurídica, de derecho público, autonomía administrativa, patrimonio propio y régimen administrativo, fiscal especial.

De acuerdo con lo establecido por la Ley 1625 de 2013, tiene dentro de sus competencias programar y coordinar el desarrollo armónico, integrado y sustentable de los municipios que la conforman; y en este contexto ha contribuido de forma activa en la conformación del territorio, mediante el liderazgo en los procesos de planificación enmarcados dentro del componente físico territorial del Plan de Desarrollo Metropolitano, estableciendo políticas, planes y proyectos de aumento, mejoramiento, cualificación, del espacio público, parques, zonas verdes y deportivas.

Por otra parte, el pasado 17 de diciembre de 2015 mediante Acuerdo Metropolitano No. 033 de 2015, se adoptó el Plan Integral de Desarrollo del Área Metropolitana de Bucaramanga "DIME TU PLAN 2016-2026", fundamentado en los principios de planeación, integración metropolitana, gobernanza metropolitana, desarrollo humano, y equidad.

El área metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura. Que sea competitiva en el nuevo mundo digital, que avanza día a día. Con ello se busca promover la implementación y ejecución de buenas prácticas de seguridad y privacidad de la información, siendo la información un activo de gran importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de esta.

El presente manual establece las políticas que integran un modelo de gestión de la seguridad dentro de la organización cuyo destino final son los usuarios internos y externos, (funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación), esto para identificar y minimizar los riesgos a los cuales se expone el uso de la información en el área metropolitana de Bucaramanga AMB, enfocándonos en el cumplimiento de la normatividad legal Colombiana Vigente ISO 27001/2013 y al modelo de seguridad y privacidad de la información (MSPI) del Ministerio de tecnologías e información y las comunicaciones de Colombia.

## 2. OBJETIVO

Establecer políticas y lineamientos de seguridad y privacidad de la información, teniendo en cuenta requisitos legales, operativos, tecnológicos, y dando cumplimiento a la concepción de seguridad en cuanto a confidencialidad, integridad, disponibilidad y autenticación de la información, determinar permitir y conocer las políticas del buen uso y administración de la información dentro de la entidad a todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación), bajo el liderazgo del área de sistemas de información y gestión corporativa

## 3. PROPOSITO

La Política de Seguridad de la Información del Área Metropolitana de Bucaramanga, es aplicable y debe ser cumplida por todos sus funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Entidad, para conseguir un nivel de protección adecuado.
Para la entidad la información es uno de sus más preciados y valiosos activos por lo tanto surge la necesidad de establecer de manera urgente los mecanismos y herramientas necesarios para su debida protección y utilización; así como también su seguimiento y mejora continua por medio de la optimización de los procesos institucionales apoyados en la concientización y el compromiso de los funcionarios acerca de los procedimientos ante cualquier eventualidad.

Tratando de mantener siempre unos altos niveles de excelencia y calidad en todos sus procesos Teniendo claro la importancia de mantener protegida su información se procede a establecer mediante este documento su Política General de Seguridad y Privacidad de la Información. En la cual estarán contenidas las directrices para la protección y seguridad de sus activos de información. Qué definimos como el conjunto de datos procesados que tienen un valor para el Área Metropolitana de Bucaramanga y se encuentran soportados física o digitalmente, creados y estructurados con principios de Confidencialidad, Integridad, Disponibilidad, Calidad, Legalidad y Seguridad.

## 4. GLOSARIO

**Activo**: (Según ISO 27001): Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección, Cada activo tiene sus características, que difieren en el estado, en materia de seguridad, en los niveles de los sub estados, confidencialidad, integridad y disponibilidad.

Podemos considerar cinco grandes tipos de activos de información, que son:

1. El entorno del Sistema de Seguridad de la Información basado en ISO 27001, que comprende a los activos y que se precisan para garantizar los siguientes niveles.
2. El sistema de información en sí.
3. La misma información generada por la aplicación del Sistema de Seguridad de la Información.
4. Las funcionalidades de la organización, en las que se justifican las exigencias de los Sistemas de Información anteriores y les generan la finalidad deseada.
5. Otros activos, ya que el tratamiento realizado a los activos es un método de evaluación de riesgos que tienen que permitir la inclusión de cualquier otro activo, sea cual sea su naturaleza

**Activo:** Cualquier cosa que tiene valor para la organización. [NTC 5411-1:2006]
**Activo de información**: Datos o información que se almacena en cualquier tipo de medio y que es considerada como sensitiva o crítica

**Adware:** Software que se apoya en anuncios como parte del propio programa. La publicidad generada es mostrada después de la instalación de dicho programa.

**Amenaza**: Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

**Antispam:** Aplicación o herramienta informática que se encarga de detectar y eliminar correo no deseado.

**Antivirus:** Software utilizado para eliminar programas elaborados con intención destructiva.

**Aplicación engañosa:** Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.

**Autenticación básica:** Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

**Armouring**: Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

**Blacklist** (Lista negra): Es un proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos

**Bots** (Red): Son grupos de ordenadores infectados controlados de forma remota por un hacker.

**Cracker:** Personas que rompen algún sistema de seguridad, (Fines de lucro, protesta o desafío)

**Cookie:** Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

**Certificado digital**: Archivo digital generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

**Correo no deseado:** cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

**Cifrado:** Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

**Control de acceso a la red (Nac**): Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas, cumplan con las políticas de seguridad establecidas para evitar amenazas.

**Ciberseguridad:** Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

**Delito Informático:** Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

**Desbordamiento de búfer:** Se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos

**Driver:** Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc.

**Encriptación:** Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer

cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas

**Exploit:** Un error en el software que representa una brecha de seguridad.

**Extorsión**: El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.

**Extensión:** Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN.

**Firewall:** Un componente de hardware o software diseñado para bloquear el acceso no autorizado

**Firma de Antivirus**: Las bases de firmas de un antivirus son el conjunto de cadenas que posee para detectar distintos códigos maliciosos. Sus actualizaciones se producen cuando el producto descarga nuevas firmas, que son incorporadas a su base para así poder detectar más amenazas.

**Freeware:** Salida no controlada de información que hace que esta llegue a personas no autorizadas

**Gateway:** Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

**Gusanos:** Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuario

**Hacker:** Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

**Hacking:** Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

**HTTP (HyperText Transfer Protocol:** Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

**Ingeniería Social**: Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

**IP (Internet Protocol) / TCP-IP**: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes.

**Keylogger:** Es un tipo de malware diseñado para capturar las pulsaciones, movimientos

y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito

**Malware:** Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

**Nuke** (ataque): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

**Pharming**: Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios

**Phishing**: Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

**Ransomware**: Programa maligno que bloquea totalmente nuestro equipo y pide dinero a cambio de devolver el control.

**Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

**Robo de datos:** Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

**Rootkits**: Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red.

**Scareware**: Hacer creer a los usuarios que el equipo está infectado, para hacer comprar una aplicación falsa.

**Spam:** También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

**Spyware:** Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas sin permiso de los usuarios

**Virus:** Programa de ordenador capaz de incrustarse en disco y replicarse repetidamente,

sin el conocimiento o permiso del usuario.

**Vulnerabilidad:** Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

**Zombie:** Ordenadores infectados controlados de forma remota por los ciberdelincuentes.

## 5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

El Área Metropolitana de Bucaramanga, en su compromiso de generar un ambiente de seguridad de información, opta por crear una política con respecto a la gestión de la seguridad de la información en función de una misión y una visión institucional que permite reducir el riesgo a una mala manipulación de la información única y confidencial, esta política una vez aprobada debe ser publicada y comunicada a todos sus funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan acceso a información a través de los documentos, equipos de cómputo e infraestructura tecnológica.

Para el Área Metropolitana de Bucaramanga, 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

### Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Área Metropolitana de Bucaramanga y la ciudadanía en general.

### Nivel de cumplimiento

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

El Área Metropolitana de Bucaramanga, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos misionales y visionales alineados con las necesidades de la institución

A continuación, se establecen los 11 principios de seguridad que soportan el SGSI para el Área metropolitana de Bucaramanga:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
2. El Área Metropolitana de Bucaramanga, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
3. El Área Metropolitana de Bucaramanga, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. El Área Metropolitana de Bucaramanga protegerá su información de las amenazas originadas por parte del personal.
5. El Área Metropolitana de Bucaramanga protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. El Área Metropolitana de Bucaramanga controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. El Área Metropolitana de Bucaramanga implementará control de acceso a la información, sistemas y recursos de red.
8. El Área Metropolitana de Bucaramanga garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. El Área Metropolitana de Bucaramanga garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. El Área Metropolitana de Bucaramanga garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
11. El Área Metropolitana de Bucaramanga garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá

consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### Estructura organizacional

El Área Metropolitana de Bucaramanga, está en proceso de crear un comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo, con el fin de garantizar el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información.

### Contratación

Los contratos o acuerdos contractuales que realice el Área Metropolitana de Bucaramanga deben incluir cláusulas que especifiquen las responsabilidades sobre el adecuado tratamiento de Información, estableciendo sanciones en caso de incumplimiento, y advirtiendo sobre la responsabilidad que en materia legal implica su desconocimiento. Se debe mantener un registro por Contratista, Proveedor, Cliente y Usuario del entendimiento y seguimiento de la Política.

### 6.1 GESTION DE ACTIVOS

En el Área Metropolitana de Bucaramanga, Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios.

El Área Metropolitana de Bucaramanga protege la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello aplica controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Él área metropolitana de Bucaramanga complementará la identificación y clasificación de los activos de información de acuerdo a su nivel de criticidad y nivel de confidencialidad. Igualmente, a definir el mecanismo para la identificación, uso, administración, protección y responsabilidad de los activos de información.

### Directrices para cumplir:

- Anualmente se deben hacer inventarios revisar y actualizar los listados de activos de información, definiendo responsabilidades, criticidad, sensibilidad, reserva,

protección adecuada. (Las fechas están sujetas a cambios solicitador por la dirección general)

- Toda la información que es generada por los funcionarios, contratistas practicantes visitantes y terceros que presten sus servicios del área metropolitana de Bucaramanga en beneficio y desarrollo de las actividades propias, se consideran activos y son propiedad del área metropolitana de Bucaramanga, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución

- Es responsabilidad de todos los Funcionarios, contratistas practicantes visitantes y terceros que presten sus servicios al área metropolitana de Bucaramanga, el hacer buen uso de dispositivos de almacenamiento externos como: (Servicios de la Nube, USB, reproductores portátiles MP3/Mp4, Discos Duros, Smartphones, Sd cards, y otros dispositivos derivados de almacenamiento), esto con el fin de facilitar el compartir y transportar información que no sea de carácter confidencial ni sensible a la entidad.

- Todos los usuarios deben devolver sus activos de información, equipos de cómputo asignados y otros implementos asignados, en buen estado, una vez cese su relación laboral o contrato con la Entidad. Será entregado por medio de la herramienta de Gestión de Recursos de TI para su reasignación de acuerdo con las necesidades,

- Implementar la gestión de riesgos sobre los activos de información, teniendo en cuenta las herramientas actuales definidas en el manual de riesgo de la entidad y adecuándolas de ser necesario para que cumplan con las guías al respecto de MINTIC

## 6.2 CONTROL DE ACCESO

- Todos los funcionarios, contratistas, practicantes, proveedores que presten un servicio al Área Metropolitana de Bucaramanga y requieran de ingresar a los sistemas de información, aplicativos, redes Inalámbricas, y otros, deben a través de su supervisor solicitar su usuario y contraseña a la Subdirección Administrativa y Financiera - Apoyo tecnológico para su respectivo tramite

- Los equipos que son propiedad del AMB, cuentan con un usuario administrador que sirve como respaldo de la información y permite controlar las aplicaciones y programas que están previamente instalados dando cumpliendo al licenciamiento

legal de software, los funcionarios y contratistas a los cuales se les otorgue un equipo computo, se asignara un usuario en Windows con acceso limitado, esto con el fin de que no se agregue software malicioso o hagan mal uso de estos equipos de información.

- Los empleados no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

- Solo el personal del Área de Sistemas y tecnología del Área Metropolitana de Bucaramanga está autorizado para acceder y realizar mantenimiento a los aplicativos, y sistemas de información o equipos tecnológicos con los que cuente la entidad.

### 6.3 NO REPUDIO

La entidad se compromete a mitigar e iniciar con el estudio de mecanismos de control de usuarios (logs) en los sistemas de información; de tal manera que quede y conste cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado, y que se haga seguimiento a los mismos, de tal manera que un usuario no pueda negar su responsabilidad sobre un cambio en los ejercicios de intercambio electrónico de la información. En la construcción de aplicaciones o sistemas de información nuevos o existentes garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

### 6.4 PRIVACIDAD Y CONFIDENCIALIDAD

Cualquier funcionario, contratista, practicantes, visitantes y terceros que presten sus servicios al Área Metropolitana de Bucaramanga que intente inhabilitar, vencer o sobrepasar los controles de seguridad de la Información en forma no autorizada será sujeto de las acciones legales correspondientes de acuerdo a la normatividad colombiana.

### 6.5 INTEGRIDAD

Cualquier funcionario o contratista practicantes visitantes y terceros debe utilizar los activos de información del área metropolitana de Bucaramanga en forma responsable, profesional, ética y legal. En particular, la entidad velará porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones ni alteraciones, al destinatario correspondiente. Igualmente, la entidad protege su información de las amenazas originadas por parte del personal.

Cualquier funcionario o contratista que tenga acceso a la información y que requiera modificar, alterar o cambiar la información de las Bases de Datos, repositorios o medios físicos (papel) debe contar con actos administrativos internos que así lo permitan o con autorización escrita por el jefe inmediato o supervisor siempre y cuando estos sean del nivel directivo.

- Mantener la privacidad de la información de las comunicaciones personales y un nivel de servicio apropiado.
- Monitorear la carga de tráfico de la red y cuando sea necesario tomar acción para proteger la integridad y operatividad de sus redes.
- La información generada y recibida de la Entidad, debe ser usada por los usuarios únicamente para los propósitos de la misionalidad de la Entidad, por las funciones propias de su cargo y para responder por información de los entes de control o terceros (previa autorización del jefe inmediato o del jefe de la dependencia responsable de la información).

## 6.6 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Entidad deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información. La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- **Niveles de disponibilidad:** Esta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.

- **Planes de recuperación:** La política debe incluir los planes de recuperación que incluyan las necesidades de disponibilidad del negocio.

- **Interrupciones:** La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad del mismo.

- **Acuerdos de Nivel de servicio:** Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.

- **Segregación de ambientes:** Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.

• **Gestión de Cambios:** La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

## 6.7 REGISTRO Y AUDITORÍA

- **Responsabilidad:** Estos procesos estarán a cargo de la oficina de sistemas de la entidad y la oficina de control interno quien tendrá la responsabilidad de hacer seguimiento para que se le dé cumplimiento a las políticas definidas por la entidad como también de informar sobre los resultados obtenidos en dichas auditorias.

- **Almacenamiento de registros:** la oficina de sistemas de la entidad estará encargada de realizar y almacenar las copias de seguridad y respaldo de las diferentes aplicaciones de la entidad para lo cual utilizará discos duros externos y se tiene previsto adquirir dispositivo tape backup para almacenamiento en cintas magnéticas.

- **Normatividad:** ***"Ley 87 de 1993****. Descripción: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".* por medio de la cual se le otorgan competencias a la oficina de control interno para ejercer estas tareas.

- **Garantía cumplimiento:** la oficina de control interno de la entidad propenderá por el análisis de los resultados obtenidos en las revisiones realizadas, garantizando el funcionamiento correcto de los sistemas de información de la entidad y realizando las debidas observaciones sobre las debilidades detectadas.

- **Periodicidad:** la entidad establece realizar controles cada (6) seis meses para analizar la efectividad medidas y los niveles de riesgos existentes.

## 6.8 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Todos los incidentes deben ser reportados a los jefes directos de cada área con copia al supervisor del departamento de sistemas para su respectivo tramite y gestión.

- Para el reporte de incidentes los usuarios cuentan correo corporativo dispuesto para la comunicación entre dependencias; además de tener a su disposición un software de gestión de procesos que les permite documentar y hacer seguimiento en tiempo real a cualquier clase de requerimiento.

-

- La entidad cuenta con un plan de privacidad y seguridad de la información y también de un plan de tratamiento de riesgos de la información.

- Todo incidente será reportado inmediatamente al personal de la oficina de sistemas, quienes a su vez harán una inspección para identificar el tipo de evento y así tomar las medidas necesarias según lo establecido en los protocolos establecidos en el plan de riesgos.

- El manejo de los incidentes debe darse de la siguiente forma el usuario que detecta el incidente, lo escala con el funcionario de sistemas, este identifica el evento , lo reporta si es necesario realiza el reporte a corser, se le informa al jefe del área de la ocurrencia del evento reportando consecuencias ,posteriormente se informa al jefe de la subdirección administrativa y financiera con copia al jefe de control interno y por ultimo si es necesario se le hace un informe detallado de lo ocurrido al director de la entidad.

## 6.9 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- La subdirección Administrativa y Financiera – Apoyo Tecnológico será la encargada de realizar divulgación de la información acerca de la seguridad de la información a través de redes sociales, correo corporativo, página web de la entidad y otros medios digitales posibles

- Realizar campañas de capacitación a todos sus funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica.

- Deben establecerse medidas de control de acceso al sistema operativo en los equipos del área metropolitana de Bucaramanga, para garantizar la autenticación de los funcionarios.

- El área metropolitana de Bucaramanga valora la información desde el punto de vista de seguridad y acorde a ello determina los mecanismos de protección adecuados.

- El área metropolitana de Bucaramanga debe informar a los funcionarios y contratistas sobre la obligatoriedad de asistir a las jornadas de capacitación programadas.

- El área metropolitana de Bucaramanga debe establecer un mecanismo que permita revisar periódicamente los resultados obtenidos luego de las

capacitaciones, de tal manera que permita retroalimentar conocimientos.

- Se deben crear los manuales y guías con respecto de los temas tratados en las capacitaciones.

- El presente documento contiene políticas adicionales que para este caso serán:

  - Política de uso aceptable.
  - Política de uso de contraseñas
  - Política De Escritorio Limpio.

## 7. VIGENCIA

Esta política tiene una vigencia indefinida y puede ser modificada o revisada periódicamente a medida que surja la necesidad y con la autorización de la secretaria General, el departamento de sistemas u oficina de tecnologías de información y aprobación de Dirección General

Todo cambio a esta política será informado oportunamente a todos los colaboradores del área metropolitana de Bucaramanga

**HISTORIA**

| FECHA | VERSIÓN | CAMBIOS |
|---|---|---|
| 30/07/2018 | 1.0 | Emisión inicial del documento |
| 20/11/2019 | 1.1 | Modificaciones del documento - Plan de mejoramiento |
| 11/08/2021 | 1.2 | Modificaciones del documento |