1. OBJETIVOS

1.1 OBJETIVO GENERAL

Determinar los lineamientos que permitan proteger la Información de la Alcaldía de Bello a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

1.2 OBJETIVOS ESPECÍFICOS

La Alcaldía de Bello, para el cumplimiento de su misión, visión, objetivos estratégicos y alineados a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas o practicantes de la Alcaldía de Bello respecto al correcto manejo y protección de la información que es gestionada y resguardada en la Alcaldía de Bello.
- Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Proteger la información y los activos tecnológicos de la Institución.
- Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la Alcaldía de Bello.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.
- Atender las necesidades para el cumplimiento de la función administrativa.
- Proteger la información y los activos tecnológicos de la Institución.
- Concientizar a los funcionarios, contratistas y practicantes de la Alcaldía de Bello sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información
- Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Línea respecto a la Seguridad de la Información.

2. ALCANCE

La Política de Seguridad de la Información aplica a todo la Alcaldía de Bello, sus funcionarios, contratistas y practicantes de la Alcaldía de Bello, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución.

3. GLOSARIO

Activo: Todo lo que tiene valor para la Alcaldía de Bello. Hay varios tipos de activos entre los que se incluyen:

- Información,
- Software, como un programa de cómputo.
- Físico, como un computador
- Servicios
- Personas, sus calificaciones, habilidades y experiencia;
- Intangibles, tales como la reputación y la imagen.

Clave: contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente. (Asimismo llamado PIN - Personal Identificación Number).

Confidencial: significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

Correo Electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la Alcaldía de Bello, para los funcionarios, contratistas y practicantes autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Custodio de la información: es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en todo la Institu con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Estrategia de Gobierno en Línea: Estrategia definida por el Gobierno Nacional que busca apoyar y homologar los contenidos y servicios ofrecidos por cada una de las entidades públicas para el cumplimiento de los objetivos de un Estado más eficiente, transparente y participativo, donde se presten servicios más eficientes a los ciudadanos a través del aprovechamiento de las tecnologías de información.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Intranet: Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

Mecanismos de bloqueo: son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como de los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información. Los bloqueos pueden ser temporales o definitivos dependiendo de tipo de situación presentada.

Memoria USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también lápiz de memoria, lápiz USB o memoria externa, siendo innecesaria la voz inglesa pen drive o pendrive.

Mensajería Instantánea Institucional: Comúnmente conocido como “Chat”, es un canal de comunicación provisto por la Alcaldía de Bello para facilitar una forma de comunicación en tiempo real entre los funcionarios, contratistas y practicantes autorizados creando un espacio virtual de encuentro específico.

Phishing (cosecha y pesca de contraseñas): Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás información confidencial.

Política: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías, las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la Institución y deben ofrecer direccionamientos a toda la Entidad o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Propietario de la información: En tecnologías de la información y la comunicación (TIC) es el responsable de preservar y disponer de la información de acuerdo a los line amientos de la Entidad. El término tecnologías de la información se usa a menudo para referirse a cualquier forma de hacer cómputo. Como nombre de un programa de licenciatura, se refiere a la preparación que tienen estudiantes para satisfacer las necesidades de tecnologías en cómputo y comunicación de gobiernos, seguridad social, escuelas y cualquier tipo de organización.

Puntos de entrada y salida: Cualquier dispositivo (distinto de la memoria RAM) que intercambie datos con el sistema lo hace a través de un "puerto", por esto se denominan también puertos de E/S ("I/O ports"). Desde el punto de vista del software, un puerto es una interfaz con ciertas características; se trata por tanto de una abstracción (no nos referimos al enchufe con el que se conecta físicamente un dispositivo al sistema), aunque desde el punto de vista del hardware, esta abstracción se corresponde con un dispositivo físico capaz de intercambiar información (E/S) con el bus de datos.

RSS (Really Simple Syndication): RSS son las siglas de Really Simple Syndication, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS tales como Internet Explorer, entre otros (agregador).

Scanner: Es un periférico que permite transferir una imagen desde un papel o superficie y transformarlos en gráficos digital (proceso también llamado digitalización). Existen actualmente escáneres que capturan objetos en tres dimensiones. Suelen utilizar un haz de luz o láser para realizar el proceso. Los escáneres no distinguen el texto de los gráficos, por lo tanto, debe existir un procesamiento de la imagen escaneada para generar texto editable. Este proceso es llamado OCR, y existen múltiples aplicaciones para tal fin. La resolución de los escáneres se mide en DPI.

Seguridad de la información: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Servicios de almacenamiento de archivos "On line": Un servicio de alojamiento de archivos, servicio de almacenamiento de archivos online, o centro de medios online es un servicio de alojamiento de Internet diseñado específicamente para alojar contenido estático, mayormente archivos grandes que no son páginas web. En general estos servicios permiten acceso web y FTP. Pueden estar optimizados para servir a muchos usuarios (como se indica con el término "alojamiento") o estar optimizados para el almacenamiento de usuario único (como se indica con el término "almacenamiento"). Algunos servicios relacionados son el alojamiento de videos, alojamiento de imágenes, el almacenamiento virtual y el copiado de seguridad remoto.

SGSI: Sistema de Gestión de Seguridad de la Información: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Sistemas de Información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Habitualmente el término se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

Smartphone: El teléfono inteligente (en inglés: smartphone) es un tipo teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional. El término
«inteligente», que se utiliza con fines comerciales, hace referencia a la capacidad de usarse como un computador de bolsillo, y llega incluso a reemplazar a una computadora personal en algunos casos.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

Tecnología de la información T.I.: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Tipos de información: cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en:

a) Documentos de Archivo (físicos y electrónicos). b) Archivos institucionales (físicos y electrónicos). c) Sistemas de Información Corporativos.
d) Sistemas de Trabajo Colaborativo.
e) Sistemas de Administración de Documentos. f) Sistemas de Mensajería Electrónica.
g) Portales, Intranet y Extranet. h) Sistemas de Bases de Datos.
i) Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc.
j) Cintas y medios de soporte (back up o contingencia). k) Uso de tecnologías en la nube.

Usuario de la información: Para la informática es un usuario aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. A menudo es un usuario aquel que adquiere una computadora o dispositivo electrónico y que lo emplea para comunicarse con otros usuarios, generar contenido y documentos, utilizar software de diverso tipo y muchas otras acciones posibles. El usuario no es necesariamente uno en particular instruido o entrenado en el uso de nuevas tecnologías, ni en programación o desarrollo, por lo cual la interfaz del dispositivo en cuestión debe ser sencilla y fácil de aprender. Sin embargo, cada tipo de desarrollo tiene su propio usuario modelo y para algunas compañías el parámetro de cada usuario es distinto.

Webcam: Cámara Web: Una cámara web o cámara de red (en inglés: webcam) es una pequeña cámara digital conectada a una computadora la cual puede capturar imágenes y transmitirlas a través de Internet, ya sea a una página web o a otra u otras computadoras de forma privada. Las cámaras web necesitan una computadora para transmitir las imágenes. Sin embargo, existen otras cámaras autónomas que tan sólo necesitan un punto de acceso a la red informática, bien sea ethernet o inalámbrico. Para diferenciarlas de las cámaras web se las denomina cámaras de red.

4. MARCO LEGAL Y/O NORMATIVO

LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292

DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf

LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-3528_documento.pdf

DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones. Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-3586_documento.pdf

DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Disponible en Línea:
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

MANUAL GOBIERNO EN LÍNEA 3.1 Ver 2014-06-12. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea; Formato Política SGSI - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

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. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf

DECRETO 103 DE 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556

DECRETO 1494 DE 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea:

http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf

5. TIPO DE POLÍTICA

Según el Decreto 2482 de 2012 "Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión" la política de seguridad de la información corresponde a las políticas de Eficiencia Administrativa.

6. POLÍTICA

La Alcaldía de Bello decide definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión y funciones de la Institución.

La Alcaldía de Bello, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites de la institución, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas, practicantes y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo.

Toda la información que es generada por los funcionarios, contratistas y practicantes la Alcaldía de Bello en beneficio y desarrollo de las actividades propias de la Institución es propiedad la Alcaldía de Bello, 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.

La La Alcaldía de Bello protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej.: contratistas, proveedores o ciudadanos), o como resultado de servicios internos en outsourcing.

La Alcaldía de Bello protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
La Alcaldía de Bello protege su información de las amenazas originadas por parte de sus funcionarios, contratistas, practicantes y usuarios.

La Alcaldía de Bello protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La Alcaldía de Bello controla la operación de sus procesos de operación garantizando la seguridad de los recursos tecnológicos, redes y bases de datos.

La Alcaldía de Bello implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos

La Alcaldía de Bello garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La Alcaldía de Bello garantiza 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.

La Alcaldía de Bello garantiza la disponibilidad de sus procesos de operación y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La Alcaldía de Bello garantiza el cumplimiento de las obligaciones legales, regulatorias contractuales establecidas.

Las responsabilidades frente a la seguridad de la información de la Institución son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes de la Institución.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad de la información siempre y cuando no sea contrario a lo expresado en esta política.

6.1. RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN Y AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

6.1.1. RESPONSABILIDADES DE LA DIRECCIÓN DE LAS TIC Y SOPORTE TECNOLÓGICO

- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la institución de acuerdo a las mejores prácticas y lineamientos de la Alcaldía de Bello y directrices del Gobierno.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Dirección General, las diferentes Direcciones y Jefaturas la Alcaldía de Bello, así como a los entes de control e investigación que tienen injerencia sobre la Institución.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Alcaldía.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio la Alcaldía de Bello.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la institución. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido.

- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la institución de acuerdo a las mejores prácticas y directrices de la Entidad y del Gobierno.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la institución.

6.1.2. RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los directores así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la Institución.

6.1.3. RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACIÓN

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 o Contrato.
- Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico- científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la institución al a red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por **la Dirección de las TIC y Soporte Tecnológico**.
- Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías de la Información.
- Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Alcaldía de Bello puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la Institución, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución.
- La Alcaldía de Bello no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

7. LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Lineamiento 1: Uso de contraseñas y usuarios
Expone las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o practicante de la Institución para obtener acceso a los sistemas de información, hardware y software propiedad la Alcaldía de Bello.

Lineamiento 2: Uso del servicio de coreo electrónico
Concientiza a los funcionarios, contratistas o practicantes de la Institución de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio.

Lineamiento 3: Uso del servicio de internet / intranet
Concientiza a los funcionarios, contratistas o practicantes de la Institución de las buenas prácticas a seguir sobre las normas de uso del servicio de Internet/Intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

Lineamiento 4: Uso de servicio de mensajería instantánea
Concientiza a los funcionarios, contratistas o practicantes de la Institución de las buenas prácticas a seguir sobre las normas y el uso del servicio de mensajería instantánea, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

Lineamiento 5: Uso de dispositivos de almacenamiento externo
Describe el uso permitido de los dispositivos de almacenamiento externo en la Alcaldía de Bello y las restricciones en su empleo al interior de la institución.

Lineamiento 6: Uso de dispositivos de captura de imágenes y/o grabación de video
Define el acceso y el uso de cámaras fotográficas, cámaras de video y demás dispositivos que permitan el registro de imágenes, fotografías y/o video en la Alcaldía de Bello.

Lineamiento 7: Uso de escritorios y pantallas despejadas

Define los mecanismos necesarios que se deben aplicar en la Alcaldía de Bello con el fin de proteger la información física residente en los escritorios y puestos de trabajo y la información digital almacenada en los computadores e infraestructura técnica a disposición de todos los funcionarios, contratistas o practicantes para el normal desarrollo de las actividades.

Lineamiento 8: Uso de dispositivos móviles (Tablets)

Define los mecanismos necesarios que se deben aplicar en la Alcaldía de Bello con el fin de proteger la información física residente en las tabletas asignadas a los funcionarios e inspectores la Alcaldía de Bello para el normal desarrollo de las actividades.

Lineamiento 9: Conexiones remotas

Define los requisitos y casos en que se concede acceso remoto a las plataformas tecnológicas de la Institución y las medidas de seguridad que se establece para la protección de la información que es accedida por este medio.

LINEAMIENTO 1: USO DE USUARIOS Y CONTRASEÑAS

La asignación de usuarios y contraseñas es un permiso que la Alcaldía de Bello otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

Presentar a todos los funcionarios y contratistas la Alcaldía de Bello responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información la Alcaldía de Bello.

Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.

Asegurar el correcto manejo de la información privada de la institución.

La asignación de credenciales: usuarios (Login o UserId) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por los directores, jefes de oficina o por los grupos de Talento Humano y Gestión Contractual.

Las cuentas de usuario son entera responsabilidad del funcionario, contratista o practicante al que se le asigne. La cuenta es para uso personal e intransferible.

Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.

De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido a **la Dirección de las TIC y Soporte Tecnológico**.

Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración de la Oficina de Tecnologías de la Información

TIPOS DE CUENTAS DE USUARIO

Todas las cuentas de acceso a las plataformas tecnológicas como a los sistemas de información y aplicaciones son propiedad de la Institución. Para efectos del presente lineamiento, se definen dos tipos de cuentas:

a. Cuenta de Usuario de Sistema de Información:

Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.

b. Cuenta de Administración de Sistema de Información:

Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente

estas cuentas están asignadas para su gestión por parte de **la Dirección de las TIC y Soporte Tecnológico**.

El Jefe de **la Dirección de las TIC y Soporte Tecnológico** deberá contar en un sobre cerrado y sellado con la lista de las contraseñas sensibles para la administración delos sistemas de información, plataformas tecnológicas y bases de datos. Esto resguardado bien sea en caja fuerte interna o en proveedor externo de custodia y protección de copias de seguridad.

Estas cuentas de usuario igualmente deben mantener las siguientes políticas:

1. Todas las contraseñas de usuarios administradores deben ser cambiadas al menos cada 3 meses.
2. Todas las contraseñas de usuario de sistema de información deben ser cambiadas al menos cada 3 meses.
3. Todas las contraseñas deben ser tratadas con carácter confidencial.
4. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
5. Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.
6. Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.
7. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
8. Se evitará el activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.

Uso apropiado de usuarios y contraseñas:

Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
Cambiar periódicamente las contraseñas de los sistemas de información o servicio tecnológicos autorizados.

Uso indebido del servicio de usuarios y contraseñas:

Permitir el conocimiento de las claves a terceros.
Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo
resguardo.

Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablets, memoriasUSB, teléfonos celulares, agendas electrónicas, etc.).
Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
Utilizar su usuario y contraseña para propósitos comerciales ajenos a la Institución.
Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red la Alcaldía de Bello.

Responsabilidades de los funcionarios, contratistas y practicantes con usuarios y contraseñas asignados
Conocer, adoptar y acatar este lineamiento.
Velar por la seguridad de la información a la que tenga acceso a través de las credenciales asignadas y a los sistemas de información autorizados para su acceso.
Cerrar totalmente su sesión de trabajo para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre laborando.
Dar aviso **la Dirección de las TIC y Soporte Tecnológico**, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

Monitoreo:

Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.
La Oficina de Tecnología podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.

LINEAMIENTO 2: USO DEL SERVICIO DE CORREO ELECTRÓNICO DE LA ALCALDÍA DE BELLO

El correo electrónico es un servicio basado en el intercambio de información a través de la red y el cual es provisto por la Alcaldía de Bello para los funcionarios, contratistas, practicantes previamente autorizados para su acceso.

Los objetivos específicos de los lineamientos para el uso del correo electrónico son:

- Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales la Alcaldía de Bello.
- Asegurar el correcto manejo de la información privada de la institución por parte de los funcionarios, contratistas o practicantes de la Institución.
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

El acceso al servicio de correo electrónico es un privilegio otorgado por la La Alcaldía de Bello a sus funcionarios, contratistas y practicantes y el mismo sobrelleva responsabilidades y compromisos para su uso.

La Alcaldía de Bello a criterio propio puede otorgar el acceso a los servicios de correo electrónico para la realización de actividades institucionales al personal de planta, contratistas y proveedores. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos. La Dirección General, Directores, Secretario General, Jefes o Coordinadores tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio.

Se encuentra disponible un acceso externo de la red corporativa a través del sitio web: https://mail.bello.gov.co/owa. Este sistema está pensado exclusivamente para aquellos funcionarios, contratistas o practicantes que por cualquier motivo, en un determinado momento, no puedan hacer uso del cliente de correo electrónico.

Las credenciales de los usuarios serán desactivadas de los sistemas de acuerdo a los procedimientos establecidos y según sea solicitado por los directores, jefes de oficina o por los grupos de Talento Humano y Gestión Contractual.

La falla consecutiva, después de cinco (5) intentos de acceso a la cuenta vía web ocasiona el bloqueo de la cuenta y esta se desbloquea automáticamente a los 30 minutos o por solicitud a la Mesa de Ayuda.

TIPOS DE CUENTAS DE CORREO ELECTRÓNICO

Todas las cuentas de correo electrónico que existen en el servicio de correo la Alcaldía de Bello son propiedad de la Institución. En el sistema de correo electrónico se consideran los siguientes tipos de cuenta de correo:

a. Cuentas personales:

Cualquier funcionario, contratista o practicante de la Institución puede ser autorizado a obtener y operar una cuenta de correo institucional para el uso diario de sus actividades laborales. En el caso de los contratistas y/o practicantes la asignación se dará con previa autorización de su jefe inmediato y siempre y cuando hayan licencias de buzones disponibles por parte de la Alcaldía de Bello.

El nombre de dicha cuenta de correo se creará con el formato x.y@bello.gov.co donde la X corresponde al primer nombre, mas el punto y, Y corresponde al primer apellido. Si dos o más personas tienen el mismo identificador de usuario se añadirá a la segunda persona y siguientes un dígito diferenciador al final de la cuenta de correo: 2, 3, 4, etc. (p.e. x.y2@bello.gov.co).

Los conflictos no aclarados por las reglas anteriores serán resueltos a criterio propio, por el administrador del sistema de correo, en acuerdo con la persona que solicita la cuenta.

En caso de combinaciones que deriven en palabras malsonantes podrá solicitarse el cambio de identificador de usuario.

Todo mensaje de correo electrónico que salga de una cuenta personal institucional debe llevar por regla general la siguiente estructura de firma, es responsabilidad del usuario su configuración y/o inclusión.

Nombres y apellidos completos del funcionario/contratista/practicante
Cargo
Dirección, Área o Grupo al cual pertenece
Correo Electrónico Institucional
Dirección: XXXXXXX, Tel: (57(indicativo Ciudad) XXXXXX Ext: XXXX Ciudad, Colombia
www.bello.gov.co

Esta información debe ir en fondo blanco, letra color negro, negrilla, el tipo de letra es Arial y el tamaño es 10.

Ejemplo:

Emerson Fitipaldi Cardona Profesional Especializado
Dirección de las TIC y Soporte Tecnológico
Emerson.cardona@bello.gov.co
Cra. 50 No.51-00 Edificio Gaspar de Rodas Código Postal: 051053,
Tel: 57 - 4 - 6047944 Ext. 1073

Antioquia. Colombia www.bello.gov.co

b. Cuentas de dependencias o de grupos de trabajo:

Estas cuentas son creadas para las necesidades de comunicación oficial, dependencias, Direcciones, Grupos de trabajo, etc. Deben ser solicitadas directamente por el jefe del área que corresponda, a través de los medios ya establecidos de la institución asignando a su vez el responsable de manejo de la misma. El nombre de la cuenta de correo se definirá con el formato documentossgc@bello.gov.co. El titular de la entidad será responsable del uso que se dé a dicha cuenta y del mantenimiento periódico de las claves de la misma.

Todo mensaje de correo electrónico que salga de una cuenta de Grupo de Trabajo debe llevar por regla general la siguiente estructura de firma, es responsabilidad del usuario responsable de su administración su configuración y/o inclusión.

Nombre del grupo.
Área o dependencia a la cual pertenece
Correo Electrónico Institucional
Cra. 50 No.51-00 Edificio Gaspar de Rodas Código Postal: 051053,
Tel: 57 - 4 - 6047944 Ext. XXXX
Antioquia. Colombia www.bello.gov.co

Esta información debe ir en fondo blanco, letra color negro, negrilla, el tipo de letra es Arial y el tamaño es 10.

c. Cuentas temporales:

Estas cuentas son creadas en forma temporal, con una vigencia definida previamente, con propósitos específicos de comunicación derivados de contratos temporales o provisionales. Estas cuentas tendrán una fecha de caducidad y se desactivarán automáticamente a su término, a menos que se solicite lo contrario. Se abrirán con una vigencia no mayor de 3 meses y podrán renovarse por periodos máximos similares.

Adicionalmente, será incluido de manera automática por el sistema, el logo vigente de la institución y la referencia al compromiso ambiental de l Institución, a criterio de la Dependencia encargada.

Todo correo electrónico que sea enviado fuera de la Alcaldía de Bello, a través de este servicio de correo, contendrá la siguiente clausula al pie de página del mensaje del mismo:

"Este correo electrónico y cualquier archivo(s) adjunto al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario(s). Si usted no es el destinatario indicado, queda notificado que la lectura, utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente. En el caso de haber recibido este correo electrónico por error, agradecemos informarnos inmediatamente de esta situación mediante el reenvío a la dirección electrónica del remitente. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinión oficial la Alcaldía de Bello."

This email and any file(s) attached to it contain confidential information that is exclusively addressed to its recipient(s). If you are not the indicated recipient, you are informed that reading, using, disseminating and/or copying it without authorization is forbidden in accordance with the legislation in effect. If you have received this email by mistake, please immediately notify the sender of the situation by resending it to their email address. The opinions contained in this message are solely those of the author and do not necessarily represent the official views of Alcaldía de Bello.

Uso apropiado de los servicios de correo electrónico la Alcaldía de Bello

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas y practicantes con acceso a este servicio.
- Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- Redactar los contenidos de un mensaje de correo electrónico de tal manera que sea serio, claro, conciso, cortés y respetuoso.
- Ingresar a las cuentas de correo de cada usuario a través de los medios que la Institución destina, que en este caso son los clientes de correo electrónico instalados en cada máquina. Cada funcionario, contratista o practicante tendrá asignada una credencial de acceso conformada por un usuario y una clave asignada por **la Dirección de las TIC y Soporte Tecnológico** a través de los procedimientos establecidos.

Uso indebido del servicio de correo electrónico la Alcaldía de Bello

- Participar en la difusión de “cartas en cadenas”, en esquemas piramidales o de propagandas dentro y fuera de la institución.
- Realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.
- Revelar o publicar cualquier información clasificada o reservada de la Alcaldía de Bello.
- Descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.
- Copiar ilegalmente o reenviar mensajes que hayan sido restringidos por parte del usuario o el emisor.
- Descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar expresiones difamatorias o groseras en contra de individuos, clientes o entidades públicas o privadas. Los mensajes enviados a través de este servicio no pueden contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no formal.
- Enviar información clasificada o reservada de la Alcaldía de Bello por medio de canales no seguros (no codificados) como es Internet y/o las cuentas de correo de uso público (gmail, hotmail, yahoo, etc.).
- El correo electrónico está sujeto a las mismas leyes, políticas y prácticas que se aplican a la utilización de otros medios de comunicación, tales como servicios telefónicos y medios impresos.
- Participar en actividades que puedan causar congestión o interrupción en los servicios de comunicación de la Alcaldía de Bello o la normal operación de los servicios de correo electrónico.
- Enviar correos SPAM de cualquier índole.
- Reenviar correos con contenido PHISING.
- Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar el correo electrónico para propósitos comerciales ajenos a la Alcaldía de Bello.
- Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de la Alcaldía de Bello
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Usar correos públicos para la recepción, envió o distribución de información pública clasificada o reservada propia de la Alcaldía de Bello.

- Configurar y conectar los clientes de correo electrónico con los sitios de redes sociales o con fuentes RSS que no sean autorizadas por la Alcaldía de Bello.
- Distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.
- Enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, .dll debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus. Este tipo de archivos serán eliminados automáticamente por el sistema de correo.
- Enviar contenidos multimedia (video o audio) con extensión .wav, .mp3, .mp4, .mpeg, .wma, .wmv, .mov, .asf, .flv ya que estos documentos son muy pesados y ralentizan la red de comunicaciones. Igualmente este tipo de archivos serán eliminados automáticamente.

El uso inapropiado o el abuso en el servicio de correo electrónico ocasionan la desactivación temporal o permanente de las cuentas. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

Envío y transferencia sobre el servicio de correo electrónico

- La capacidad del buzón del servidor de correo de cada funcionario, contratistas o practicante es de X (por definir)GB incluyendo la papelera de reciclaje y mensajes enviados; la de los Directores, y Jefes de Oficina es de X(por definir) GB y la de usuarios VIP es de X(por definir) GB. En determinadas ocasiones es necesario que los usuarios liberaren espacio en el buzón de correo, eliminando los correos que ya no sean necesarios, copiando los mensajes al buzón local y descargando los anexos a su computadora institucional.
- Una vez superada la cuota asignada por usuario los mensajes no pueden ser descargados a sus buzones locales hasta no liberar el espacio necesario del servidor de correo. Se notifica a cada usuario con un mensaje cuando esté próximo a completar esta cuota.
- El tamaño máximo de cada mensaje de correo electrónico no debe exceder los 20 MB para envió y 50 MB para recepción debido a las limitaciones propias de los buzones. Esto tiene efecto tanto para el envío como para la recepción e incluye los archivos adjuntos.
- El máximo número de destinatarios, en los campos Para: CC: (con copia) y CCO: (con copia oculta) para un mensaje de correo es de 40 usuarios. Si se requiere enviar a un mayor número de destinatarios al definido se debe solicitar los

permisos al administrador del servicio de correo electrónico **La Dirección de las TIC y Soporte Tecnológico.**

- Se recomienda el uso del campo CCO: para mantener la privacidad de los correos electrónicos de los destinatarios. Este campo hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista ni ser visibles a los demás.
- Los correos masivos institucionales que por necesidades específicas de un departamento o área requieran ser enviados a una parte o toda la institución, deben ser enviados a través de las cuentas departamentales creadas para tal fin. Igualmente se debe solicitar que estos correos no sean contestados por parte de los destinatarios debido a que puede provocar lentitud en el canal de comunicación o tergiversar el objetivo de la información con comentarios adicionales.
- Es una buena práctica comprimir los archivos a enviar a través de este servicio, para disminuir las exigencias técnicas en su transmisión.
- Si un mensaje no se puede entregar al destinatario (problemas de conexión, servicio no disponible, etc.) permanecerá pendiente de entrega durante un máximo de 24 horas. Pasado este plazo se le enviará al remitente un mensaje de error indicando el motivo por el que no se pudo realizar la entrega.
- Los mensajes destinados a dominios (cuentas) no válidas se rechazan inmediatamente para evitar que direcciones erróneas (por ejemplo, mal escrito) sean aceptadas por el servidor como válidas.
- Se aplican políticas de filtrado de mensajes para evitar en la medida de lo posible la llegada de correo no deseado (SPAM) a los buzones de los usuarios.
- Un mensaje no se acepta cuando provenga de un servidor identificado como fuente de SPAM o como un servidor no válido para el envío de correo electrónico por alguna de las listas de bloqueo.
- Se aplican políticas de filtrado de mensajes entrantes y salientes, rechazando el envío/recepción de mensajes que contengan virus. Cuando un mensaje es rechazado se envía una notificación al destinatario del mensaje, salvo en el caso de virus que falsifique el emisor del mensaje.
- Un adjunto se borra cuando, a través de los procesos automáticos de evaluación, sea identificado como portador de virus o cualquier otra amenaza para el destinatario, comunicándole al mismo este hecho mediante un mensaje al pie del correo electrónico.

Responsabilidades de los funcionarios, contratistas y practicantes que sean usuarios de los servicios de correo electrónico de la Alcaldía de Bello

- Cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de la Política de la Institución.
- Usar correctamente las credenciales de ingreso (usuario y clave) asignadas. La cuenta de correo que proporciona la Institución es personal e intransferible, por lo que no debe compartirse con otras personas.
- Cerrar totalmente la sesión de lectura y envío de correos para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre configurada la cuenta de correo.
- Dar aviso la Dirección de las TIC y Soporte Tecnológico, a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.
- Responsabilizarse por la información o contenido que sea transmitido a través de la cuenta de correo asignada; Los usuarios del servicio deben considerar que los mensajes enviados a un destinatario pueden ser re-enviados a cualquier número de cuentas de correo de otros individuos o grupos.
- Descargar, verificar y resguardar la información recibida a través de este servicio en su buzón local de correo electrónico, de ser este configurado, en el cliente de correo instalado en su equipo de cómputo.

Monitoreo

La Alcaldía de Bello tiene el derecho a acceder y revelar los contenidos electrónicos de los correos electrónicos institucionales de sus funcionarios, contratistas y practicantes y estos deben dar su consentimiento a la Alcaldía de Bello en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.

El Administrador del Servicio **la Dirección de las TIC y Soporte Tecnológico** pueden monitorear en línea el acceso y uso de los servicios Institucionales, o revisar el contenido de los equipos e información Institucional almacenados en cualquier momento, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad dela información; Igualmente se efectúa una revisión periódica del tráfico de mensajes sobre los canales de comunicación como prevención de ingreso de mensajes tipo SPAM o PHISING, ingreso de virus sobre las redes y equipos informáticos, verificación de volúmenes de archivos anexos que puedan afectar la operación del sistema.

La Dirección de las TIC y Soporte Tecnológico pueden monitorear el cumplimiento de las directrices institucionales en el momento que así lo considere o le sea requerido, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad del sistema.

LINEAMIENTO 3: USO DELSERVICIO DE INTERNET/INTRANET DE LA ALCALDÍA DE BELLO

Los objetivos específicos del uso de servicio de internet/intranet son:

- Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales la Alcaldía de Bello.
- Asegurar el correcto manejo de la información privada de la Institución.
- Garantizar la confidencialidad, la privacidad y de uso adecuado y moderado dela información a través de este servicio.

El servicio de Internet/Intranet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas de cómputo interconectados en red a nivel local y mundial.

El acceso al servicio de Internet/Intranet es un permiso otorgada por la Alcaldía de Bello a sus funcionarios, contratistas o practicantes y así mismo sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

Cada Secretario, Director, Jefe o Coordinador de área tiene la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio, de acuerdo al procedimiento vigente.

El ingreso a este servicio se realiza por medio de la plataforma que la **Alcaldía de Bello** destina, que para este caso es el navegador de internet instalado en cada máquina.

El punto de inicio para acceder a este servicio se hace desde la página web institucional a través de la dirección: http://www.bello.gov.co.

Uso apropiado del servicio de Internet/Intranet

Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso indebido del servicio de Internet/Intranet:

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.
- Acceder y/o descargar material pornográfico u ofensivo.
- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por **la Dirección de las TIC y Soporte Tecnológico**.
- Compartir en sitios web información propia la Alcaldía de Bello clasificada como reservada o clasificada sus usuarios, funcionarios, contratistas o practicantes.
- Emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada la Alcaldía de Bello a través de servicios y cuentas de correo públicos.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a la Alcaldía de Bello.

- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por la Alcaldía de Bello.
- Interferir intencionalmente con la operación normal de cualquier website o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizara el acceso a aquellos funcionarios, contratistas o practicantes que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la autorización ante **la Dirección de las TIC y Soporte Tecnológico**.

- Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la **Alcaldía de Bello** dirigidos a funcionarios, contratistas o practicantes y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- Descargar, instalar y configurar navegadores distintos a los permitidos por **la Dirección de las TIC y Soporte Tecnológico.**

Responsabilidades de los Usuarios de Internet/Intranet en la Alcaldía de Bello:

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.
- Usar correctamente sus credenciales de ingreso (usuario y clave).
- La cuenta de acceso que proporciona la **Alcaldía de Bello** es personal e intransferible, por lo que no debe proporcionarse a otras personas.
- Dar aviso **la Dirección de las TIC y Soporte Tecnológico** a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, pérdida de la contraseña, bloqueo, etc.
- Proteger los derechos de autor de la información obtenida a través de este servicio. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este medio.

Monitoreo:

- Los funcionarios, contratistas y practicantes deben estar al tanto que se registra por cada usuario las visitas a los diferentes sitios y se registra estos eventos en archivos de auditoria tanto en los computadoras, propias o contratadas, como en los servidores donde se administran estos servicios.
- **La Dirección de las TIC y Soporte Tecnológico** planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas y navegación en Internet-Intranet.
- Si se determina que alguna de las páginas previamente restringidas por **la Dirección de las TIC y Soporte Tecnológico** es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo y con el visto bueno de **la Dirección de las TIC y Soporte Tecnológico**.
- Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PHISING) por lo que se recomienda confirmar esta

información directamente con las mismas entidades. Igualmente no se debe proveer información personal ni laboral a sitios de dudosa validez. La Alcaldía de Bello no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

LINEAMIENTO 4: USO DELSERVICIO MENSAJERÍA INSTANTÁNEA

El acceso al servicio de mensajería instantánea es un permiso otorgada por la **Alcaldía de Bello** a sus funcionarios, contratistas o practicantes y la misma sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios conserven normas de buen uso, confidencialidad y criterio ético.

Los objetivos específicos del uso de servicio de mensajería instantánea son:

- Incentivar el uso del servicio de mensajería instantánea para fines estrictamente laborales de la **Alcaldía de Bello.**
- Asegurar el correcto manejo de la información privada de los usuarios y de la institución
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado del mismo.

- Este servicio es suministrado para los funcionarios, contratistas y practicantes, previamente autorizados para su uso, con el propósito de agilizar el trato entre los mismos a lo largo y ancho de la entidad, independiente de su ubicación física o geográfica.

- Este servicio es una potente herramienta para realizar conferencias virtuales además de permitir compartir el escritorio del computador como las aplicaciones residentes en el mismo. Su uso es recomendado para presentaciones en tiempo real, entrenamientos remotos, web conferencias y reuniones en línea.

- El ingreso a este servicio se realiza por medio de la plataforma que **la Dirección de las TIC y Soporte Tecnológico** destina para este caso por medio del software

instalado en cada máquina y/o a través del navegador de internet residente en cada computador.

- Como todo servicio, que basa su operación en el manejo de información, la **Alcaldía de Bello** promueve el uso prudente y mesurado de este servicio para apoyar las operaciones y comunicaciones propias de la Institución.

Uso apropiado del servicio de Mensajería Instantánea:

- Usar el servicio de mensajería instantánea institucional exclusivamente para fines laborales.
- Transferir archivos que no tengan información sensible o reservada de la **Alcaldía de Bello**. Se debe revisar previamente que cualquier archivo a enviar esté libre de virus.
- Abstenerse de compartir información o datos personales a través de este servicio. No es aconsejable incluir información personal como contraseñas o números de tarjetas de crédito, cuentas bancarias e incluso un número de teléfono en cierta manera confidencial.
- Compartir por medio de este canal mensajes concisos, breves y veraces.
- Mantener su estado actualizado en el sistema de modo que los demás usuarios sepan si están o no disponibles y si pueden o no contactarle.

Uso indebido del servicio de mensajería instantánea:

- Emplear el servicio de mensajería instantánea Institucional para extensas conversaciones personales.
- Expresar opiniones difamatorias, ofensivas, obscenas, vulgar, racistas, calumniadoras y sexuales sobre superiores, compañeros o subalternos. Lo mismo aplica para usuarios, proveedores y demás entidades con quien haya comunicación. Esto puede comprometer la reputación y su credibilidad tanto de índole personal como institucional.
- Emplear las comunicaciones instantáneas con fines políticos, religiosos o comerciales.
- Realizar cualquier tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.

- Compartir por medio de este canal información clasificada o reservada de la **Alcaldía de Bello**, de sus funcionarios, contratistas o practicantes
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Compartir documentos o archivos que sean ajenos a la operación de la institución. Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los clientes de mensajería instantánea instalados por la **Alcaldía de Bello**.
- Descargar, instalar y emplear sistemas de mensajería instantánea distintos al definido por La Alcaldía de Bello y administrado por **la Dirección de las TIC y Soporte Tecnológico**. Los sistemas no autorizados incluyen pero no se limitan a: Yahoo! Messenger, AOL Instant Messenger (AIM), MSN Messenger, Whatsapp, eBuddy, ICQ, MySpace y Google Talk.
- El uso inapropiado o el abuso en el servicio de mensajería instantánea ocasionaran la desactivación temporal o permanente de las cuentas.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios del servicio de mensajería instantánea:

- Conocer, adoptar y acatar este lineamiento cada vez que haga uso de este servicio.
- Usar correctamente sus credenciales de ingreso (usuario y clave). La cuenta de acceso que proporciona la institución es personal e intransferible, por lo que no debe proporcionarse a otras personas.
- Dar aviso **la Dirección de las TIC y Soporte Tecnológico** a través de los medios establecidos de cualquier fallo de seguridad de su cuenta, incluyendo su uso no autorizado, olvido de la contraseña, bloqueo, etc.
- Todos los mensajes compartidos y documentos archivos compartidos o descargados quedan bajo responsabilidad del dueño de la cuenta.
- Cada jefe de área es responsable de revisar y autorizar o desautorizar cada requerimiento de acceso de sus funcionarios, contratistas o practicantes a este servicio. Solicitudes aprobadas de acceso deben ser sometidas de acuerdo con el procedimiento vigente para este caso.
- Los usuarios del servicio deben considerar que los mensajes instantáneos pueden ser guardados por su interlocutor. Una de las partes que participa en la conversación puede copiar y pegar la conversación entera en un documento de texto. Este servicio de mensajería instantánea permiten incluso archivar mensajes completos

Monitoreo:

- Los funcionarios, contratistas o practicantes deben estar al tanto de que se registra por cada usuario los mensajes y llamadas enviadas y recibidas en archivos de auditoria tanto en los computadoras, propias o contratadas, como en los servidores donde se administran estos servicios.
- **La Dirección de las TIC y Soporte Tecnológico** planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas.

LINEAMIENTO 5: USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

El uso de medios de almacenamiento externo a los disponibles en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la entidad, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, contratistas o practicantes de la Institución que a la vez puede exponer información confidencial y sensible de la entidad a diversos riesgos y peligros.

Los objetivos específicos del uso de dispositivos de almacenamiento externo son:

- Concientizar a los funcionarios, contratistas o practicantes de la institución sobre los riesgos asociados con el uso de los medios de almacenamiento, tanto para los sistemas de información como para la infraestructura tecnológica de la Entidad.
- Asegurar el correcto manejo de la información digital que reposa en la institución.
- Delimitar el uso de estos medios de almacenamiento en las diferentes áreas de la **Alcaldía de Bello**.

- La **Alcaldía de Bello** es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón la **Alcaldía de Bello** define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

- El uso de dispositivos de almacenamiento externo está permitido en la **Alcaldía de Bello** para los funcionarios, contratistas y practicantes; en general los funcionarios,

contratistas o practicantes de la Institución, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la Institución dentro de las normas y responsabilidades del manejo de información institucional.

- Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo de la **Alcaldía de Bello**. Entre estos, se pueden encontrar pero no se limitan a:

    1. Memorias Flash USB
    2. Reproductores portátiles MP3/MP4
    3. Cámaras con conexión USB
    4. iPhones/Smartphones
    5. SD Cards/ Mini SD Cards/ Micro SD Cards.
    6. Tablets
    7. Dispositivos con tecnología Bluetooth.
    8. Tarjetas Compact Flash
    9. Discos duros de uso externo

Nota: El acceso y empleo de servicios de almacenamiento de archivos On Line, es decir, aquellas unidades virtuales de almacenamiento personal por medio de internet, en las cuales se incluye pero no se limitan los servicios de Skydrive, Dropbox, Rapidshare, GigaSize, MediaFire, 4shared, etc.; están prohibidos.

Uso indebido de dispositivos de almacenamiento externo:

- Almacenar o transportar información clasificada o reservada de la **Alcaldía de Bello**.
- Ejecutar cualquier tipo de programa no autorizado por la Institución desde cualquiera de las unidades de almacenamiento en mención.
- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.
  Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, contratistas o practicantes de la Institución.

En concordancia con lo anterior, queda RESTRINGIDO el uso de Dispositivos de Almacenamiento Externo, en las siguientes dependencias(definir donde)

- Secretaría de Servicios Administrativos
- Grupo Gestión Documental y Correspondencia
- Tesoreria

La Dirección de las TIC y Soporte Tecnológico pueden en todo momento y en cualquier área o dependencia de la Institución operar, almacenar, adquirir o retirar dispositivos de almacenamiento externo que les permita garantizar la seguridad de la información la **Alcaldía de Bello**.

Responsabilidades de los usuarios de dispositivos de almacenamiento externo:

- Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.
- Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Institución por medio del software de protección dispuesto para tal fin.

Monitoreo:

- Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la institución, podrán ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y el usuario que los empleó. Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido denegado o no autorizado igualmente podrán ser registrados.
- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas al administrador de la red de la Institución.
- Se pueden generar informes periódicos sobre el uso de todos los elementos en la **Alcaldía de Bello** para permitir la evaluación del "uso racional de los dispositivos" y que estos sean permitidos, a fin de incrementar los niveles de seguridad para proteger la información de la Institución.

LINEAMIENTO 6: USO DE DISPOSITIVOS DE CAPTURA DE IMÁGENES Y/O GRABACIÓN DE VIDEO

Los objetivos específicos del uso de dispositivos de captura de imágenes y/o grabación de video son:

- Concientizar a los funcionarios, contratistas, practicantes y demás personas vinculadas con la institución sobre los riesgos asociados al uso de dispositivos de registros de imagen y/o video, en las instalaciones de la Institución.
- Fortalecer las medidas de seguridad en las áreas de la **Alcaldía de Bello**, que gestionan documentos e información de la Institución.
- Dar cumplimiento a las directrices determinadas en la Política de Seguridad de la Información de la institución.
- Restringir el uso de este tipo de dispositivos en áreas de manejo de información y documentación clasificada o reservada.

Entre los dispositivos de captura de imágenes y/o grabación de video se pueden encontrar pero no se limitan a:

1. Cámaras Fotográficas
2. Videocámaras
3. Celulares.
4. iPhones/Smarthphones
5. Tablets.
6. WebCams
7. Scanners
8. Impresoras
9. Multifuncionales

Nota: La captura de imágenes y/o grabación de video por parte de los ciudadanos o visitantes de la Entidad está prohibida.

No se permite la captura de imágenes y/o grabación de video en las instalaciones o sedes la **Alcaldía de Bello**, así como del personal por parte de la ciudadanía, funcionarios, contratistas y practicantes de la Institución, sin previa autorización de la **Secretaría de Servicios Administrativos**.

El acceso y uso de equipos fotográficos y de video para fines Institucionales, prensa o de comunicación a la **Alcaldía de Bello** debe ser autorizado previamente.

No se permite la captura de imágenes y/o grabación de video bajo ninguna circunstancia en las siguientes dependencias:

(DEFINIR LUGARES)

Con el único propósito de brindar protección en las áreas anteriormente descritas, del personal, documentos, información y activos en estas áreas alojados, los únicos dispositivos de registro audiovisual permitidos son las cámaras de seguridad que la Institución designe.

En el caso de equipos de cómputo la **Alcaldía de Bello** que cuenten con webcams integradas y los dispositivos de videoconferencia su uso es exclusivo para videoconferencias institucionales al interior de las dependencias y áreas antes señaladas.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios de dispositivos de captura de imágenes y/o grabación de video:

- Adoptar, poner en práctica, socializar, y acatar estos lineamientos.
- Usar los dispositivos de captura de imágenes y/o grabación de videos que sean de su propiedad o le hayan sido asignadas para el desempeño de sus actividades de acuerdo a lo estipulado anteriormente.
- Abstenerse de fotografiar, escanear, grabar o copiar digitalmente información sensible, clasificada o reservada de la Institución.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estos lineamientos o si conocen de alguna falta a alguna de ellas.

Monitoreo:

- La **Alcaldía de Bello** puede controlar el acceso de dispositivos de captura de imágenes y/o grabación de video a sus instalaciones en las entradas a cada una de sus sedes a nivel nacional, por medio del personal de vigilancia y seguridad dispuesto en cada uno de los puntos de ingreso de la entidad.
- El monitoreo permanente de uso y manipulación de dispositivos de captura de imágenes y/o grabación de video, es efectuado a través de los sistemas de video vigilancia instalados en las diferentes áreas y sedes de la Institución.
- La **Alcaldía de Bello** requerirá y mantendrá bajo custodia del personal de vigilancia y seguridad los dispositivos de captura de imágenes y/o grabación de video en las

dependencias restringidas y determinadas en esta Política a cualquier persona que ingrese a las mismas y durante el tiempo que permanezca al interior de las mismas.

LINEAMIENTO 7: USO DE ESCRITORIOS Y PANTALLAS DESPEJADAS

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas y practicantes la **Alcaldía de Bello** y apoya en la seguridad de la información sensible o crítica de la Institución.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.
- Dictar las pautas para mantener organizado y resguardado los documentos digitales y correos electrónicos en los computadores puestos a disposición de todos los usuarios de los sistemas de información y estructura tecnológica de la **Alcaldía de Bello**.

Este lineamiento se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante de la Institución y pantalla, el área de trabajo virtual sobre el sistema operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información la Alcaldía de Bello, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

Escritorios:

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.
- Se debe evitar el retiro de documentos clasificados o reservados de la institución y en el caso de ser necesario se debe propender por su protección fuera de la Institución y su pronta devolución al mismo.
- Se deben controlar la recepción, flujo envío de documentos físicos en la Institución por medio de registro de sus destinatarios desde el punto de correspondencia.
- Se debe restringir el fotocopiado de documentos fuera del horario normal de trabajo y fuera de las instalaciones de la Institución. De ser necesario se debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad fuera.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.
- No se debe enviar ni recibir documentos clasificados o reservados por medio de Fax.
- No se debe reutilizar papel que contenga información clasificada o reservada.

Pantallas:

- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.
- Las áreas de trabajo virtuales “pantallas” del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.
- Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.
- Los funcionarios, contratistas y practicantes al retirarse de la Institución deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y estaciones de trabajo utilizados para acceso remoto.
- Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.

- **La Dirección de las TIC y Soporte Tecnológico** determinan una configuración automática en todos los equipos de cómputo, propiedad o contratados por la Institución, para que se active el protector de pantalla del computador, bloqueando el acceso al computador al presentarse una inactividad de 15 minutos. Estos pueden ser nuevamente utilizados por los usuarios al volver a realizar la autenticación por medio de los usuarios y contraseñas asignados.
- El fondo de pantalla de cada computador es único para todos las estaciones de trabajo y para todos los usuarios y puede ser cambiado únicamente por l **la Dirección de las TIC y Soporte Tecnológico** o por solicitud la **Oficina Asesora de Comunicaciones**. Para el resto de las áreas, estos cambios deben ser solicitados y validados por la **Oficina Asesora de Comunicaciones.**

Monitoreo:

La Dirección de las TIC y Soporte Tecnológico en conjunto con la **Secretaría de Servicios Administrativos**, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

LINEAMIENTO 8: USO DE DISPOSITIVOS MÓVILES (TABLETS)

La política de uso de dispositivos móviles (tablets) aplica a todos los funcionarios, contratistas y practicantes del La **Alcaldía de Bello** y apoya en la seguridad de la información sensible o crítica del Institución.

Los objetivos específicos de este capítulo relacionado con el uso de dispositivos móviles son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información a través de las Tablets y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener tanto los dispositivos como la información protegida.
- Dictar las pautas para mantener la operación, y transmisión de la información registrada en las tablets.

Responsabilidades de la Dirección de las TIC y Soporte Tecnológico:

- Determinar y avalar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por la institución.
- Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por la Alcaldía de Bello.
- Determinar los métodos de protección de acceso (por ejemplo, contraseñas o patrones) para los dispositivos móviles institucionales que serán entregados a los usuarios.
- Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Implementar una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo.
- instalar un software de antivirus en los dispositivos móviles institucionales que hagan uso de los servicios provistos por la institución.
- Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Responsabilidades de los usuarios:

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Aceptar y aplicar la nueva versión de las actualizaciones que sean notificadas en los dispositivos móviles asignados para su uso.
- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Abstenerse de almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados

Monitoreo:

La Dirección de las TIC y Soporte Tecnológico en conjunto con la **Secretaria de Servicios Administrativos,** sin previo aviso, realizan brigadas de monitoreo para verificar el estado de la tablets y generar el respectivo informe de lo encontrado.

LINEAMIENTO 9: CONEXIONES REMOTAS

La política de conexiones remotas es extensiva para todos los funcionarios, contratistas y practicantes la Alcaldía de Bello que requieran y les sea autorizado el acceso a terminales o servidores institucionales a través de herramientas VPN para el desarrollo de sus actividades en horarios fuera de los normales o desde ubicaciones diferentes a las oficinas de la Alcaldía de Bello.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al acceso y gestión de información sobre las plataformas institucionales de manera remota y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener segura la información y los elementos utilizados para el acceso y operación remota de información.
- Dictar las pautas para mantener organizado y resguardado las credenciales de acceso así como los elementos de protección para asegurar la conexión remota.

-

Responsabilidades de La Dirección de las TIC y Soporte Tecnológico:

- Establecer e implementar los métodos de conexión remota a la plataforma tecnológica de la **Alcaldía de Bello**.
- Implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica Institucional.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la **Alcaldía de Bello** de manera permanente.

Responsabilidades de los usuarios:

- Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la **Alcaldía de Bello** y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Mantener en total reserva las direcciones de entrada a las direcciones Institucionales (direcciones ip o direcciones Web) al igual que las credenciales que les han sido otorgadas para su resguardo.
- Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones Institucionales.
- Aplicar herramientas de antivirus sobre sus computadores personales, en lo posible, para brindar una mayor protección a los archivos e información que están gestionando.
- Dar aviso **la Dirección de las TIC y Soporte Tecnológico** de cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

Monitoreo:

La Dirección de las TIC y Soporte Tecnológico en conjunto con la **Secretaria de Servicios Administrativos**, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de las conexiones remotas, así como el tiempo y uso efectuado a través de este medio y generar el respectivo informe de lo encontrado.

8. DOCUMENTO DE APROBACIÓN

Se debe realizar reunión con el comité del GEL para discutir políticas y en este punto escribir el numero del acta con su fecha respectiva de la aprobación.