POLÍTICA DE SEGURIDAD DE LA INFOMACIÓN

SUBSECRETARÍA DE GESTIÓN TICS Y DOCUMENTAL

SUBSECRETARIO: JAMES CORDOBA QUINTO

AUTOR: ALEJANDRO ALMARIO RINCÓN

ALCALDÍA DE APARTADO

2022

1. Objetivo

Establecer las políticas que regulan la seguridad de la información en la alcaldía de Apartadó y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los directivos, funcionarios, contratistas, proveedores, practicantes, visitantes, usuarios y terceros que presten sus servicios o tengan algún tipo de relación con la alcaldía de Apartadó.

2. Alcance.

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas, proveedores, practicantes, visitantes, usuarios y terceros que presten sus servicios o tengan algún tipo de relación con la alcaldía de Apartadó, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Todos los usuarios internos y externos tienen la obligación de dar cumplimiento a las presentes políticas emitidas.

3. Campo de Aplicación.

Este manual aplica para todos los procesos que se gestionan al interior de la Administración Municipal.

4. Responsables.

Son responsables de la aplicación de este documento el Alcalde, Representante de la Dirección, Secretarios de despacho, gerentes, jefes y demás servidores y particulares que ejerzan funciones públicas a nombre de la Administración Municipal de Apartadó.

5. Términos y Definiciones:

5.1. Acción Correctiva: Conjunto de acciones tomadas para eliminar la(s) causa(s) de no una conformidad detectada u otra situación no deseable.

5.2. Acción Preventiva: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

5.3. Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

5.4. Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

5.5. Administración de Riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo. Las estrategias incluyen transferir el riesgo a otra parte, evitar el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

5.6. Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se

basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- ✓ Detectar cualquier alteración en los servicios TI.
- ✓ Registrar y clasificar estas alteraciones.
- ✓ Asignar el personal encargado de restaurar el servicio.

5.7. **Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

5.8. **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

5.9. **Amenaza**: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

5.10. **Análisis de riesgos:** Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

5.11. **Auditabilidad:** Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

5.12. **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

5.13. **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

5.14. **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

5.15. **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

5.16. **Base de datos de gestión de configuraciones (CMDB, Configuration Management Database):** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

5.17. **BS7799:** Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable- Asimismo la parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO

27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

5.18. Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

5.19. Checklist o lista de Chequeo: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

5.20. CobiT - Control Objectives for Information and related Technology – (Objetivos de Control para la información y Tecnologías Relacionadas): Publicados y mantenidos por ISACA, sus siglas en inglés (Information System Audit And Control Association) – Asociación de Auditoría y Control de Sistemas de Información Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

5.21. Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

5.22. Computo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

5.23. Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

5.24. Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

5.25. Control: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

5.26. Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

5.27. Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

5.28. Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

5.29. Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

5.30. Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de

su selección como de la exclusión de controles incluidos en el anexo A de la norma.

5.31. Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

5.32. Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

5.33. Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

5.34. Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

5.35. Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

5.36. Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

5.37. Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

5.38. Gestión de claves: Controles referidos a la gestión de claves criptográficas.

5.39. Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

5.40. Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

5.41. Impacto: Resultado de un incidente de seguridad de la información.

5.42. Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

5.43. Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

5.44. Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la entidad o faciliten información con

clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

5.45. Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

5.46. Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

5.47. IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

5.48. ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

5.49. ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.

5.50. ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

5.51. ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

5.52. ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de julio de 2007.

5.53. ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

5.54. ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

5.55. ISO/IEC TR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

5.56. ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

5.57. Keyloggers: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

5.58. Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

5.59. No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

5.60. No conformidad grave o mayor: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

5.61. No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

5.62. PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

5.63. Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra

información bancaria), mediante una aparente comunicación oficial electrónica.

5.64. Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que ponga en peligro el funcionamiento de este.

5.65. Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

5.66. Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

5.67. Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

5.68. Riesgo Residual: Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

5.69. Salvaguarda: Véase: Control.

5.70. Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

5.71. Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además,

otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

5.72. SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]: es un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

5.73. Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

5.74. Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

5.75. Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

5.76. Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

5.77. Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

5.78. Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

5.79. Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en

descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

5.80. Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. Políticas de Operación.

a. El Manual de la Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.
b. Este documento debe ser parte de todo proceso de inducción y/o reinducción de los servidores públicos y particulares que realicen o vayan a realizar funciones públicas a nombre de la Administración.
c. Este documento debe ser la base para definir criterios de control de la seguridad de la información en el cumplimiento de la gestión de los procesos de la Administración.
d. Es responsabilidad de todos los servidores públicos y particulares que ejercen funciones públicas a nombre de la Administración Municipal de Apartadó, cumplir con las disposiciones dadas en este documento.
e. Es responsabilidad del Representante de la Dirección, del Consejo de Gobierno y la Subsecretaría de TIC la actualización de este.

7. Contenido.

7.1. Política general de seguridad de la información.

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

La Alcaldía de Apartadó, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía de Apartadó
- ✓ Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad:

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Alcaldía de Apartadó y la ciudadanía en general.

Nivel de cumplimiento:

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

A continuación, se establecen las 26 políticas de seguridad que soportan el SGSI de La Alcaldía de Apartadó:

- ✓ La Alcaldía de Apartadó ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- ✓ La Alcaldía de Apartadó protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- ✓ La Alcaldía de Apartadó protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ La Alcaldía de Apartadó protegerá su información de las amenazas originadas por parte del personal.

- ✓ La Alcaldía de Apartadó protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ La Alcaldía de Apartadó controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ La Alcaldía de Apartadó implementará control de acceso a la información, sistemas y recursos de red.
- ✓ La Alcaldía de Apartadó garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ La Alcaldía de Apartadó garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ La Alcaldía de Apartadó garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- ✓ La Alcaldía de Apartadó garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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

7.2. Política de Estructura Organizacional de Seguridad de la Información:

La Alcaldía de Apartadó creará un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información.

Objetivo:

Definir el programa de seguridad de la información en donde se describan roles y responsabilidades para operación, gestión y administración de seguridad de la información.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Crear el Comité de Seguridad de la Información, y asignar el rol de Oficial de seguridad de la información y su equipo de apoyo, junto con los roles, funciones y responsabilidades respectivamente.
- ✓ La Subsecretaría TIC y Gestión Documental debe establecer roles, funciones y responsabilidades de operación y administración de los sistemas de información a los funcionarios, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.
- ✓ La Subsecretaría TIC y Gestión Documental asistirá a foros, conversatorios, conferencias de interés especial en seguridad de la información.

7.3. Política para uso de dispositivos móviles

Objetivo:

Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “Smart Phones”, tabletas, entre otros), suministrados por la entidad y personales que hagan uso de los servicios de información.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.
- ✓ Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual.
- ✓ Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Almacén Municipal.
- ✓ Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.
- ✓ Es responsabilidad del usuario hacer buen uso del dispositivo suministrado con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.

7.4. Política de seguridad para los recursos humanos

Objetivo:

Asegurar que los funcionarios, contratistas y demás colaboradores de la Alcaldía de Apartadó, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Se debe asegurar que los funcionarios, contratistas y demás colaboradores de la Alcaldía de Apartadó, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información
- ✓ Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación a la Alcaldía de Apartadó para el tratamiento de sus datos personales de acuerdo a la Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- ✓ El Área de Talento Humano deberá verificar la competencia necesaria de los candidatos o aspirantes a ocupar la vacante disponible.
- ✓ A la firma del contrato laboral o posesión del cargo el funcionario debe firmar un acuerdo de confidencialidad para con la Alcaldía de Apartadó.
- ✓ Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.
- ✓ Los funcionarios deben cumplir con el manual de Excelencia Ética y Buen Gobierno.
- ✓ En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

7.5. Política de uso de los activos

Objetivo:

Lograr y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Los activos de información pertenecen a la Alcaldía de Apartadó y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- ✓ Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área de TIC.
- ✓ EL Área de TIC proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Alcaldía de Apartadó, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes
- ✓ Periódicamente, el Área de TIC efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de la Alcaldía de Apartado.

- ✓ Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el funcionario encargado del bien y si es contratista, o practicante atreves Jefe de la dependencia a través de la Mesa de Ayuda del Área de TIC.
- ✓ Estarán bajo custodia del Área de TIC los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las claves de administración de los equipos informáticos, sistemas de información o aplicativos.
- ✓ Los recursos informáticos no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política o cualquier otro uso que no esté autorizado.
- ✓ Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
- ✓ Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de TIC:

  - ➢ Instalar software en cualquier equipo de la Alcaldía de Apartadó.
  - ➢ Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la Alcaldía de Apartadó.
  - ➢ Modificar, revisar, transformar o adaptar cualquier software propiedad de la Alcaldía de Apartadó;

- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Alcaldía de Apartadó.
- Copiar o distribuir cualquier software o licencia de propiedad de la Alcaldía de Apartadó.
- Cambiar la configuración del hardware de propiedad de la Alcaldía de Apartadó.

- ✓ El usuario deberá informar al Área de TIC de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la Alcaldía de Apartadó que tenga conocimiento.
- ✓ El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
- ✓ Ningún usuario deberá acceder a la red o a los servicios TIC de la Alcaldía de Apartadó, utilizando una cuenta de usuario o clave de otro usuario.
- ✓ Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos.
- ✓ Todos los archivos provenientes de equipos externos a la Alcaldía de Apartadó, deben ser revisados para detección de virus antes de su utilización en la red.
- ✓ Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios del Área de TIC.
- ✓ La información de la Alcaldía de Apartadó debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
- ✓ Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados en el proceso de desvinculación, de igual manera

deberán documentar y entregar los conocimientos importantes que posee de la labor que ejecutan.

7.6. Política de uso de estaciones cliente.

Objetivo:

Garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ La instalación de software en los computadores suministrados, es una función exclusiva del Área de TIC.
- ✓ Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.
- ✓ Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.
- ✓ En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
- ✓ Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente y deberán ubicar copias y documentos finales en las carpetas

virtuales centralizadas que se establezcan para cumplir con las tablas de retención documental TRD de la Entidad.

- ✓ El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá de acuerdo a la disponibilidad.
- ✓ Los equipos que ingresan temporalmente a la Alcaldía de Apartadó que son de propiedad de terceros: deben ser registrados en los controles de acceso de la entidad para poder realizar su retiro; posteriormente de la Alcaldía de Apartadó no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
- ✓ El Área de TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Alcaldía de Apartadó.

7.7. Política de uso de Internet.

Objetivo:

Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de la Alcaldía de Apartadó, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso la información.
- ✓ La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- ✓ No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Alcaldía de Apartadó que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la Alcaldía de Apartadó. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del subsecretario de TIC.
- ✓ La Subsecretaría TIC y Gestión Documental, administrará autorización de navegación a los usuarios de la Alcaldía de Apartadó, previa solicitud del Jefe de la dependencia.
- ✓ La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

7.8. Política de control de acceso

Objetivo:

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de la Alcaldía de Apartadó, así como el uso de medios de computación móvil.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red estas claves de acceso y usuarios son personales e intransferibles.
- ✓ El comité de seguridad de la Información establecerá el listado software autorizado para uso en los sistemas de información y comunicaciones.
- ✓ Solo usuarios designados por el Área de TIC estarán autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Alcaldía de Apartadó, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software malicioso.
- ✓ Todo trabajo a realizarse en los servidores con información de la entidad, por parte de sus funcionarios o contratistas, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del Subsecretario de TIC.
- ✓ La conexión remota a la red de área local debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

7.9. Política de establecimiento, uso y protección de claves de acceso.

Objetivo:

Controlar el acceso a la información.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Se debe concienciar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario.
- ✓ Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.
- ✓ Los usuarios deben tener en cuenta los siguientes aspectos:

  - ➢ El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
  - ➢ Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
  - ➢ Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por tres veces.
  - ➢ La clave de acceso será desbloqueada luego de la solicitud formal por parte del responsable de la cuenta.

- ✓ Las claves o contraseñas deben:
  - ➢ Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
  - ➢ Nunca utilice sus contraseñas personales en el entorno laboral
  - ➢ Tener mínimo 8 caracteres alfanuméricos.

- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente cada 6 meses, o cuando lo establezca el Área de TIC.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos. No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal del Área del TIC.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

7.10. Política de uso de discos de red o carpetas virtuales.

Objetivo:

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Para que los usuarios tengan acceso a la información ubicada en los discos de red, el jefe inmediato deberá enviar a la mesa de ayuda del Área de TIC, el acceso y permisos correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red.

- ✓ La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
- ✓ La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
- ✓ Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.
- ✓ Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
- ✓ Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
- ✓ La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Área de TIC.
- ✓ La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de la Alcaldía de Apartadó, estará a cargo del Área de TIC.

7.11. Política de uso de puntos de red de datos (red de área local – LAN).

Objetivo:

Asegurar la operación correcta y segura de los puntos de red.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la información.

Directrices:

- ✓ Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.
- ✓ Los equipos de uso personal, que no son de propiedad de la Alcaldía de Apartadó, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Área de TIC.
- ✓ La instalación, activación y gestión de los puntos de red es responsabilidad del Área de TIC.

7.12. Política de uso de impresoras y del servicio de Impresión.

Objetivo:

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la Alcaldía de Apartadó.

Directrices:

- ✓ Los documentos que se impriman en las impresoras de la Alcaldía de Apartadó deben ser de carácter institucional.
- ✓ Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- ✓ Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda del Área de TIC.
- ✓ Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

7.13. Política de Seguridad Física

Objetivo:

Implementar el programa de seguridad física para el acceso a las instalaciones, centros de datos y centros de cableado que permita fortalecer la integridad, disponibilidad e integridad la información

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la Alcaldía de Apartadó.

Directrices:

- ✓ La Secretaria General es la encargada debe implementar un sistema de seguridad física para las instalaciones de la Alcaldía de Apartadó.
- ✓ El Área de TIC debe implementar barreras y sistemas de control de acceso a las instalaciones, centros de datos y centros de cableado.
- ✓ El Área de TIC debe implementar alarmas de detección de intrusos a los centros de datos y centros de cableado.
- ✓ La Secretaria General, implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para

prevenir inundaciones o humedad en los centros de datos y centros de cableado.

- ✓ El Área de TIC, deberá implementar protecciones que eviten ó mitiguen daños causados por incendios, inundaciones y otros desastres naturales o generados por el hombre a los centros de datos y centros de cableado.

7.14. Políticas de seguridad del centro de datos y centros de cableado.

Objetivo:

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la Alcaldía de Apartadó.

Directrices:

- ✓ No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- ✓ El Área de TIC deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía

- ✓ La limpieza y aseo del centro de datos estará a cargo de la Secretaria General y debe efectuarse en presencia de un funcionario y/o contratista del Área de TIC. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza.
- ✓ En las instalaciones del centro de datos o de los centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales inflamables o combustibles que generen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

El centro de datos debe estar provisto de:

- ✓ Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- ✓ Pisos elaborados con materiales no combustibles.
- ✓ Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- ✓ Unidades de potencia ininterrumpida UPS, que proporcionen respaldo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- ✓ Alarmas de detección de humo y sistemas automáticos de extinción de fuego. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada año.
- ✓ Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- ✓ El cableado de la red debe ser protegido de interferencias.
- ✓ Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

- ✓ La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada y esta debe ser exclusivamente con fines institucionales.
- ✓ Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario.
- ✓ Las puertas del centro de datos deben permanecer cerradas.
- ✓ Cuando se requiera realizar alguna actividad sobre algún rack, este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- ✓ Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

7.15. Políticas de seguridad de los Equipos

Objetivo:

Asegurar la protección de la información en los equipos.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios de la Alcaldía de Apartadó.

Directrices:

- ✓ Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras.
- ✓ A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada.

- ✓ La secretaria general del debe implementar sistemas redundantes de alimentación eléctrica, como, por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía.
- ✓ Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- ✓ Deben existir planos que describan las conexiones del cableado.
- ✓ El acceso a los centros de cableado (Racks), debe estar protegido.
- ✓ El Área de TIC establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.
- ✓ la Alcaldía de Apartadó debe mantener contratos de soporte y mantenimiento de los equipos críticos.
- ✓ Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas.
- ✓ Los equipos que requieran salir de las instalaciones de la Alcaldía de Apartadó para reparación o mantenimiento, deben estar debidamente autorizados.
- ✓ Los equipos retirados de la entidad deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos.
- ✓ Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Área de TIC, así mismo se debe garantizarse la eliminación de toda información.
- ✓ La Alcaldía de Apartadó, no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica.
- ✓ El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la Alcaldía de Apartadó (consultores, pasantes, visitantes, etc.) será

registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.

- ✓ Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la perdida y/o hurto.

7.16. Política de escritorio y pantalla limpia.

Objetivo:

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ El personal de la Alcaldía de Apartadó, debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- ✓ El personal de la Alcaldía de Apartadó debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- ✓ Los usuarios de los sistemas de información y comunicaciones de la Alcaldía de Apartadó, deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- ✓ Los usuarios a los que la Alcaldía de Apartadó les asigne equipos móviles como computadores, teléfonos inteligentes, tablets, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.
- ✓ Al imprimir documentos con información pública reservada y/o pública clasificada (semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- ✓ La información pública reservada o información pública clasificada (privada o semiprivada) que se encuentre en medio físico, debe permanecer almacenada en gabinete de seguridad.

7.17. Política de adquisición, desarrollo y mantenimiento de sistemas de información.

Objetivo:

Garantizar que la seguridad es parte integral de los sistemas de información.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad de la información.
- ✓ El Área de TIC deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- ✓ El Área de TIC desarrollará y/o adquirirá el software requerido por la Alcaldía de Apartadó; de manera coordinada con el Área que manifieste la necesidad del software, el Área de TIC establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.
- ✓ Se debe verificar que los desarrollos de la entidad estén completamente documentados, igualmente todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo externa a la entidad.
- ✓ Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de la Alcaldía de Apartadó, por cualquier dependencia o proyecto, deberá ser gestionado por el Área de TIC para su correcto funcionamiento.
- ✓ La compra de licencia de un programa permitirá a la Alcaldía de Apartadó, realizar una copia de seguridad, para ser utilizada en caso de que el medio se averíe.

- ✓ Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización con lleva a las sanciones administrativas y legales pertinentes.
- ✓ En los equipos de la Alcaldía de Apartadó solo se podrá utilizar el software licenciado.
- ✓ Para la adquisición y actualización de software, es necesario efectuar la solicitud al Área de TIC con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- ✓ Se encuentra prohibido el uso e instalación de juegos en los computadores.

7.18. Política de respaldo y restauración de información.

Objetivo:

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ La información de cada sistema debe ser respaldada sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, etc.
- ✓ Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y

los requerimientos de seguridad de la información; de igual manera, es el responsable de realizar los respaldos periódicos.

- ✓ Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- ✓ Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
- ✓ Debe ser desarrollado un plan de emergencia para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- ✓ Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
- ✓ Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones.
- ✓ La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
- ✓ Semanalmente se verificará la correcta ejecución de los procesos de backup.
- ✓ El Área de TIC debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas.
- ✓ Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que se entrega a los usuarios.

7.19. Política para realización de copias en estaciones de trabajo de usuario final.

Objetivo:

Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad pública correspondiente, en este caso la Alcaldía de Apartadó, son de propiedad de ésta con las excepciones que la misma ley han señalado.
- ✓ En el evento de retiro de un funcionario o traslado de dependencia, previa notificación de la Subsecretaría de Talento Humano, la Subsecretaría TIC y Gestión Documental generará una copia de la información contenida en el equipo asignado al perfil del usuario, a una unidad de almacenamiento.
- ✓ En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar a la mesa de ayuda de la Subsecretaría TIC y Gestión Documental.
- ✓ Ningún usuario debe utilizar un equipo diferente al asignado para copiar algún tipo de archivo, excepto al autorizado por jefe inmediato.

7.20. Política de uso de correo electrónico.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la Alcaldía de Apartadó, en el servicio y uso del servicio de correo electrónico por parte de los usuarios autorizados.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.

- ✓ Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- ✓ Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la Alcaldía de Apartadó, se consideran bajo el control de la entidad.
- ✓ Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada y no debe utilizarse para ningún otro fin.
- ✓ No está autorizado el envío de cadenas de correo.
- ✓ No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

- ✓ Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la Alcaldía de Apartadó, su cuenta de correo será desactivada.
- ✓ Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo, la Subsecretaría de Talento Humano y la oficina encargada de la Contratación son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas a La Subsecretaría TIC y Gestión Documental.
- ✓ Las cuentas de correo electrónico son propiedad de la Alcaldía de Apartadó, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, en comisión permanente, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad y no debe utilizarse para ningún otro fin.
- ✓ Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.
- ✓ Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
- ✓ Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@apartado.gov.co con la frase “correo sospechoso” en el asunto.
- ✓ El único servicio de correo electrónico autorizado en la entidad es el asignado por la Subsecretaría TIC y Gestión Documental.

Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:

El contenido de este mensaje y sus anexos son propiedad de la Alcaldía de Apartadó, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal.
Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo sistemas@apartado.gov.co.

7.21. Políticas específicas para funcionarios y contratistas del Área de TI.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información de la Alcaldía de Apartadó por parte de los funcionarios, practicantes y contratistas de TI de la entidad.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ El personal del Área de TI no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Jefe de la Subsecretaría TIC y Gestión Documental.
- ✓ Los usuarios y claves de los administradores de sistemas y del personal del Área de TI son de uso personal e intransferible.
- ✓ El personal del Área de TI debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.
- ✓ Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- ✓ Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- ✓ Los funcionarios del Área de TI no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Subsecretario de TI y el registro en el sistema de la mesa de ayuda.
- ✓ Los funcionarios del Área de TI se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- ✓ Los funcionarios del Área de TI de Información no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
- ✓ Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- ✓ Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad.

- ✓ El acceso a cualquier servicio, servidor o sistema de información debe ser autorizado.

7.22. Política para la Gestión de la Continuidad de Seguridad de la Información.

Objetivo:

Asegurar la continuidad de la seguridad de la información en situaciones de crisis o desastres

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ La alcaldía de Apartadó establecerá el Plan de Continuidad del Negocio para la entidad, este debe incluir el plan de recuperación de desastres.
- ✓ Se debe generar el plan de continuidad de seguridad de la información, documentado e implementando procesos y procedimientos para asegurar la continuidad requerida por la Entidad.
- ✓ El Área de TI elaborará el plan de recuperación de desastres para los sistemas de información y comunicación, el cual debe incluir mínimo procedimientos, condiciones de seguridad, recuperación y retorno a la normalidad.
- ✓ El plan de continuidad del negocio de la entidad se debe verificar, revisar y evaluar, por la Oficina de Control Interno durante el desarrollo del plan anual de auditorías.

- ✓ La Alcaldía de Apartadó propenderá por la implementación de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad necesarios para la Entidad, así como programación y ejecución de pruebas de funcionalidad de esta.

7.23. Políticas específicas para usuarios de la Alcaldía de Apartadó.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información del Alcaldía de Apartadó por parte de los usuarios de la entidad.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ La Alcaldía de Apartadó suministra una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado, esta información será guardada durante un máximo de 2 años; es de aclarar que el usuario final deberá copiar la información necesaria en la carpeta destinada para este fin la cual tiene un acceso directo en el escritorio del PC con el nombre de su usuario.
- ✓ La Alcaldía de Apartadó instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas

para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que ésta práctica no está autorizada.

- ✓ Todo el software usado en la plataforma tecnológica de La Alcaldía de Apartadó debe tener su respectiva licencia y acorde con los derechos de autor.
- ✓ La Alcaldía de Apartadó no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
- ✓ El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe hacer con moderación.
- ✓ Los programas instalados en los equipos, son de propiedad de La Alcaldía de Apartadó, la copia no autorizada de programas o de su documentación, implica una violación a la política general de La Alcaldía de Apartadó. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el La Alcaldía de Apartadó o las sanciones que especifique la ley.
- ✓ La Alcaldía de Apartadó se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los

programas de propiedad de la entidad. Se incluirá valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

- ✓ Los recursos tecnológicos y de software asignados a los funcionarios de La Alcaldía de Apartadó son responsabilidad de cada funcionario.
- ✓ Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información institucional.
- ✓ Los usuarios solo tendrán acceso a los datos y recursos autorizados por la Alcaldía de Apartadó, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- ✓ Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc.
- ✓ Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.
- ✓ Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la mesa de ayuda del Área de TI.

7.24. Política de uso de mensajería instantánea y redes sociales.

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

- ✓ El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- ✓ No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
- ✓ La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador, que sea creado a nombre personal en redes sociales como: Twitter®, Facebook®, Youtube® ,Likedink®, blogs, Instagram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
- ✓ Toda información distribuida en las redes sociales que sean originadas por la entidad deben ser autorizadas por los jefes de área o el jefe de comunicaciones para ser socializadas y con un vocabulario institucional.
- ✓ No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

7.25. Política de tratamiento de datos personales.

Objetivo: Establecer los lineamientos para administración y tratamiento de datos personales en la Alcaldía de Apartadó.

Aplicabilidad:

Estas políticas aplican a la Alta Dirección, Subsecretarios, Funcionarios, Contratistas y en general a todos los usuarios que manejen información de la Alcaldía de Apartadó.

Directrices:

Finalidades y tratamiento al cual serán sometidos los datos personales: Los datos personales que la Alcaldía de Apartadó recolecte, almacene, use, circule y suprima, serán utilizados para alguna de las siguientes finalidades:

- ✓ En relación con la naturaleza y las funciones propias de la Alcaldía de Apartadó: El Tratamiento de los datos se realizará con la finalidad de la atender y generar datos históricos, estadísticas en cumplimiento a la naturaleza de las funciones.
- ✓ En relación con el funcionamiento de la Alcaldía de Apartadó
  - ➢ Recurso Humano:

    El Tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, (incluye, entre otros, funcionarios, exfuncionarios, judicantes, practicantes y aspirantes a cargos).

  - ➢ Proveedores y Contratistas:

    El Tratamiento de los datos se realizará para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o

servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.

- Seguridad en instalaciones de la Alcaldía de Apartadó:
  El Tratamiento se realizará para seguridad de las personas, los bienes e instalaciones de gobierno bajo la responsabilidad de la Alcaldía de Apartadó.

✓ Derechos de los titulares:

- Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada a la Alcaldía de Apartadó como responsable y encargado del tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Ser informado por la Alcaldía de Apartadó como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a los datos personales del Titular.
- Presentar ante la Alcaldía de Apartadó quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Alcaldía de Apartadó haya determinado que en

el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

- ✓ Datos sensibles: El Titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la Alcaldía de Apartadó, relacionada, entre otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.
- ✓ Datos de menores de edad: El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor.

- ✓ Autorización del titular: Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

- ✓ Casos en que no se requiere la autorización:

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por Alcaldía de Apartadó en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

- ✓ Atención de peticiones, consultas y reclamos:

  Para realizar peticiones, consultas o reclamos con el fin de ejercer los derechos a conocer, actualizar, rectificar, suprimir los datos o revocar la autorización otorgada, el Titular o sus causahabientes pueden utilizar cualquiera de los siguientes canales de comunicación:

Dirección: Calle 104B No 106 - 20, Apartadó., Colombia.
Horario de atención: De lunes a jueves en el horario de atención al público (7:00 A.M. a 12:00 A.M. y de 2:00 P.M. a 5:00 P.M.) y viernes en el horario de atención al público (7:00 A.M. a 12:00 A.M. y de 2:00 P.M. 4:00 PM) Conmutador: Tel: (574) 8280457
Correo electrónico: contactenos@apartado.gov.co

- ✓ Procedimiento para ejercer los derechos:

- ➢ Consultas

Se absolverán en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible responder la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su solicitud, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

- ➢ Reclamos

Los Titulares o sus causahabientes que consideren que la información contenida en una base de datos de la entidad debe ser objeto de corrección, actualización

o supresión, o que adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante la Alcaldía de Apartadó, a través de cualquiera de los canales de comunicación descritos anteriormente; y éste deberá contener la siguiente información:

- Nombre e identificación del Titular.
- La descripción precisa y completa de los hechos que dan lugar al reclamo.
- La dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite.
- Los documentos y demás pruebas que se pretendan hacer valer.

En caso de que la Alcaldía de Apartadó no sea competente para resolver el reclamo presentado ante la misma, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

Si el reclamo resulta incompleto, la Alcaldía de Apartadó requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el peticionario presente la información solicitada, se entenderá que ha desistido de aquél.

Una vez recibido el reclamo completo, la Alcaldía de Apartadó incluirá en la respectiva base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda se mantendrá hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo, y si no fuere posible responder en dicho término, la Alcaldía de Apartadó informará al interesado los motivos de la demora y la fecha en que aquél se atenderá, sin llegar a superar, en ningún caso, los ocho (8) días hábiles siguientes al vencimiento del primer término.

- Fecha de entrada en vigencia de la política de tratamiento de la información y periodo de vigencia de las bases de datos de la Alcaldía de Apartadó:

La presente política rige a partir de su expedición y las bases de datos sujetas a tratamiento se mantendrán vigentes mientras ello resulte necesario para las finalidades establecidas en el punto 2 de la misma.

7.26. Proceso Disciplinario

Dentro de la estrategia de seguridad de la información de la Alcaldía de Apartadó, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores, violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Gestión del Talento Humano.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por la Alcaldía de Apartadó:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo a la Subsecretaría TIC y Gestión Documental.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recepcionar o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.

- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Alcaldía de Apartadó.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos para beneficio personal.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de la Alcaldía de Apartadó, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la Alcaldía de Apartadó, el que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Alcaldía de Apartadó a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de la Alcaldía de Apartadó o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Alcaldía de Apartadó.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.

- Sustraer de las instalaciones de la Alcaldía de Apartadó, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Alcaldía de Apartadó o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de la Alcaldía de Apartadó.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Alcaldía de Apartadó.
- Copiar sin autorización los programas de la Alcaldía de Apartadó, o violar los derechos de autor o acuerdos de licenciamiento.

8. Puntos de Control.

a. Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de la Alcaldía de Apartadó. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Alcaldía de Apartadó tomará las acciones disciplinarias y legales correspondientes.
b. Comunicación eficaz de las responsabilidades y autoridades de cada tipo de políticas para la ejecución segura de los procesos del SGI.

9. Documentos de Referencia.

9.1. Documentos Externos:

- ✓ Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- ✓ Código Penal Colombiano - Decreto 599 de 2000
- ✓ Ley 906 de 2004, Código de Procedimiento Penal.
- ✓ Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- ✓ Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- ✓ Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- ✓ Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- ✓ Ley 594 de 2000 - Ley General de Archivos.
- ✓ Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- ✓ Ley 527 de 1999, por 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.
- ✓ Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- ✓ Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- ✓ Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- ✓ Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- ✓ Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- ✓ Ley 1581 de 2012, "Protección de Datos personales".
- ✓ Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- ✓ Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- ✓ Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- ✓ Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas”.
- ✓ Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”.
- ✓ Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- ✓ Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- ✓ Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- ✓ Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- ✓ CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- ✓ CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- ✓ Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- ✓ Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.

- ✓ ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- ✓ Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- ✓ Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental".

10. Registros.

- Ver tabla de retención documental

11. Notas de Cambio.

12. Anexos.

Sin Anexos